United States General Accounting Office

GAO

May 2004

TECHNOLOGY ASSESSMENT

Cybersecurity for Critical Infrastructure Protection

GAO

Accountability * Integrity * Reliability

GAO-04-321

May 2004

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-321, a report to congressional requesters

TECHNOLOGY ASSESSMENT

Cybersecurity for Critical Infrastructure Protection

Why GAO Did This Study

Computers are crucial to the operations of government and business. Computers and networks essentially run the critical infrastructures that are vital to our national defense, economic security, and public health and safety. Unfortunately, many computer systems and networks were not designed with security in mind. As a result, the core of our critical infrastructure is riddled with vulnerabilities that could enable an attacker to disrupt operations or cause damage to these infrastructures. Critical infrastructure protection (CIP) involves activities that enhance the security of our nation's cyber and physical infrastructure. Defending against attacks on our information technology infrastructure—cybersecurity—is a major concern of both the government and the private sector. Consistent with guidance provided by the Senate's Fiscal Year 2003 Legislative Branch Appropriations Report (S. Rpt. 107-209), GAO conducted this technology assessment on the use of cybersecurity technologies for CIP in response to a request from congressional committees. This assessment addresses the following questions: (1) What are the key cybersecurity requirements in each of the CIP sectors? (2) What cybersecurity technologies can be applied to CIP? (3) What are the implementation issues associated with using cybersecurity technologies for CIP, including policy issues such as privacy and information sharing?

www.gao.gov/cgi-bin/getrpt?GAO-04-321.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Keith Rhodes at (202) 512-6412 or rhodesk@gao.gov.

What GAO Found

Many cybersecurity technologies that can be used to protect critical infrastructures from cyber attack are currently available, while other technologies are still being researched and developed. These technologies, including access control technologies, system integrity technologies, cryptography, audit and monitoring tools, and configuration management and assurance technologies, can help to protect information that is being processed, stored, and transmitted in the networked computer systems that are prevalent in critical infrastructures.

Although many cybersecurity technologies are available, experts feel that these technologies are not being purchased or implemented to the fullest extent. An overall cybersecurity framework can assist in the selection of technologies for CIP. Such a framework can include (1) determining the business requirements for security; (2) performing risk assessments; (3) establishing a security policy; (4) implementing a cybersecurity solution that includes people, processes, and technologies to mitigate identified security risks; and (5) continuously monitoring and managing security. Even with such a framework, other demands often compete with cybersecurity. For instance, investing in cybersecurity technologies often needs to make business sense. It is also important to understand the limitations of some cybersecurity technologies. Cybersecurity technologies do not work in isolation; they must work within an overall security process and be used by trained personnel. Despite the availability of current cybersecurity technologies, there is a demonstrated need for new technologies. Long-term efforts are needed, such as the development of standards, research into cybersecurity vulnerabilities and technological solutions, and the transition of research results into commercially available products.

There are three broad categories of actions that the federal government can undertake to increase the use of cybersecurity technologies. First, it can take steps to help critical infrastructures determine their cybersecurity needs, such as developing a national CIP plan, assisting with risk assessments, and enhancing cybersecurity awareness. Second, the federal government can take actions to protect its own systems, which could lead others to emulate it or could lead to the development and availability of more cybersecurity technology products. Third, it can undertake long-term activities to increase the quality and availability of cybersecurity technologies in the marketplace.

Ultimately, the responsibility for protecting critical infrastructures falls on the critical infrastructure owners. However, the federal government has several options at its disposal to manage and encourage the increased use of cybersecurity technologies, research and develop new cybersecurity technologies, and generally improve the cybersecurity posture of critical infrastructure sectors.

Contents

Letter 1

Technology Assessment Overview 3

Background 5
Results in Brief 7

Chapter 1 **Introduction** 18

Critical Infrastructure Protection Policy Has Evolved since the Mid-1990's 19
Federal and Private Sector Computer Security Is Affected by Various Laws 21
Report Overview 22

Chapter 2 **Cybersecurity Requirements of Critical Infrastructure Sectors** 23

Threats, Vulnerabilities, Incidents, and the Consequences of Potential Attacks Are Increasing 23
Critical Infrastructures Rely on Information Technology to Operate 37
Sectors Have Similar Cybersecurity Requirements but the Specifics Vary 42

Chapter 3 **Cybersecurity Technologies and Standards** 44

Cybersecurity Technologies 44
Cybersecurity Standards 52

Chapter 4 **Cybersecurity Implementation Issues** 58

A Risk-Based Framework for Infrastructure Owners to Implement Cybersecurity Technologies 59
Considerations for Implementing Current Cybersecurity Technologies 76
Critical Infrastructure Sectors Have Taken Actions to Address Threats to Their Sectors 86
Federal Government Actions to Improve Cybersecurity for CIP 95

Chapter 5 **Summary** 121

Agency Comments and Our Evaluation 123
External Review Comments 124

Appendix I **Technology Assessment Methodology** 126

Appendix II **Summary of Federal Critical Infrastructure Protection Policies** 129

Appendix III **Cybersecurity Technologies** 139

Overview of Network Systems 139
Access Controls 147
System Integrity 170
Cryptography 174
Audit and Monitoring 185
Configuration Management and Assurance 195

Appendix IV **Comments from the Department of Homeland Security** 208

Appendix V **Comments from the National Science Foundation** 209

Appendix VI **GAO Contacts and Acknowledgments** 211

GAO Contacts 211
Acknowledgments 211

Bibliography 212

Tables

Table 1: Critical Infrastructure Sectors Defined in Federal CIP Policy 7
Table 2: Common Cybersecurity Technologies 8
Table 3: Cybersecurity Research That Needs Continuing Attention 10
Table 4: Policy Options and Examples of Current or Planned Federal Activities to Improve Critical Infrastructure Cybersecurity 13

Table 5: Critical Infrastructure Sectors Identified by the Federal Government 20
Table 6: Threats to Critical Infrastructure 24
Table 7: Likely Sources of Cyber Attacks According to Respondents to the CSI/FBI 2003 Computer Crime and Security Survey 25
Table 8: Weapons for Physically Attacking Critical Infrastructures 27
Table 9: Types of Cyber Attacks 29
Table 10: Common Types of Current Cybersecurity Technologies 45
Table 11: Examples of Cybersecurity Standards 54
Table 12: Estimated Costs of Recent Worm and Virus Attacks 99
Table 13: Critical Infrastructure Sector-Specific Agencies 101
Table 14: Typical Research Areas Identified in Research Agendas 113
Table 15: Sampling of Current Research Topics 114
Table 16: Sampling of Long-Term Research Areas 119
Table 17: Federal Government Actions Taken to Develop CIP Policy 129
Table 18: Critical Infrastructure Sectors Identified by the National Strategy for Homeland Security and HSPD-7 137
Table 19: Cybersecurity Technology Control Categories and Types 147

Figures

Figure 1: Information Security Incidents, 1995-2003 33
Figure 2: Security Vulnerabilities, 1995-2003 34
Figure 3: An Example of Typical Networked Systems 39
Figure 4: An Overall Framework for Security 60
Figure 5: Five Steps in the Risk Management Process 62
Figure 6: Protection, Detection, and Reaction Are All Essential to Cybersecurity 67
Figure 7: Technology, People, and Process Are All Necessary for Cybersecurity 79
Figure 8: An Example of Typical Networked Systems 140
Figure 9: TCP/IP Four-layer Network Model 143
Figure 10: A Typical Firewall Protecting Hosts on a Private Network from the Public Network 150
Figure 11: How a Web Filter Works 157
Figure 12: An Example of Fingerprint Recognition Technology Built into a Keyboard 162
Figure 13: An Example of Fingerprint Recognition Technology Built into a Mouse 162
Figure 14: A Desktop Iris Recognition System 163

Figure 15: Example of a Time-Synchronized Token 166
Figure 16: Example of a Challenge-Response Token 167
Figure 17: Encryption and Decryption with a Symmetric Algorithm 175
Figure 18: Encryption and Decryption with a Public Key Algorithm 176
Figure 19: Creating a Digital Signature 180
Figure 20: Verifying a Digital Signature 181
Figure 21: Illustration of a Typical VPN 182
Figure 22: Tunneling Establishes a Virtual Connection 184
Figure 23: Typical Operation of Security Event Correlation Tools 191
Figure 24: Typical Network Management Architecture 199
Figure 25: Example of a Vulnerability Scanner Screen 204

Abbreviations

ABA	American Bankers Association
AMS	Automated Manifest System
ANSI	American National Standards Institute
ASTM	American Society for Testing and Materials
CERT/CC	CERT Coordination Center
CIA	Central Intelligence Agency
CIAO	Critical Infrastructure Assurance Office
CIDX	Chemical Industry Data Exchange
CIP	critical infrastructure protection
CMVP	Cryptographic Module Validation Program
CPU	central processing unit
CVE	Common Vulnerabilities and Exposures
DARPA	Defense Advanced Research Projects Agency
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council
FTP	File Transfer Protocol
GPS	Global Positioning System

HIPAA	Health Insurance Portability and Accountability Act
HSPD-7	Homeland Security Presidential Directive 7
HTTP	Hyper Text Transfer Protocol
I3P	Institute for Information Infrastructure Protection
IP	Internet Protocol
IAIP	Information Analysis and Infrastructure Protection
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IPS	intrusion prevention system
ISAC	information sharing and analysis center
ISP	Internet service provider
IT	information technology
LAN	local area network
NAS	National Academy of Sciences
NERC	North American Electric Reliability Council
NFS	Network File System
NIAP	National Information Assurance Partnership
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NNTP	Network News Transfer Protocol
NSA	National Security Agency
NSF	National Science Foundation
OSTP	Office of Science and Technology Policy
PC	personal computer
PDD 63	Presidential Decision Directive 63
PIN	personal identification number
PKI	public key infrastructure
POP	Post Office Protocol
R&D	research and development
RADIUS	Remote Authentication Dial-In User Service
RAM	random access memory
RFC	Request for Comments
ROM	read-only memory
SCADA	Supervisory Control and Data Acquisition
SDLC	system development life cycle
SEMATECH	Semiconductor Manufacturing Technology
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	secure sockets layer
ST-ISAC	Surface Transportation Information Sharing and Analysis Center
TACACS+	Terminal Access Controller Access System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTIC	Terrorist Threat Integration Center
UDP	User Datagram Protocol

VPN	virtual private network
WAN	wide area network

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 28, 2004

Congressional Requesters

Consistent with guidance provided by the Senate's Fiscal Year 2003 Legislative Branch Appropriations Report (Senate Report 107-209), you asked us to conduct a technology assessment on the use of cybersecurity technologies for critical infrastructure protection. This report discusses several current cybersecurity technologies and possible implementations of these technologies for the protection of critical infrastructure against cyber attacks. Potential actions to increase the availability and use of cybersecurity technologies are discussed. Key considerations for the implementation of these actions by infrastructure owners and the federal government are also discussed.

We are sending copies of this report to the Secretary of Homeland Security, the Director of the National Science Foundation, and interested congressional committees. We will provide copies to others on request. In addition, the report is available on GAO's Web site at http://www.gao.gov.

If you have questions concerning this report, please contact Keith Rhodes at (202) 512-6412, Joel Willemssen at (202) 512-6408, or Naba Barkakati, Senior Level Technologist, at (202) 512-4499. We can also be reached by e-mail at rhodesk@gao.gov, willemssenj@gao.gov, and barkakatin@gao.gov, respectively. Major contributors to this report are listed in appendix VI.

Keith A. Rhodes
Chief Technologist
Director, Center for
Technology and Engineering

Joel Willemssen
Managing Director
Information Technology

List of Congressional Requesters

The Honorable Susan M. Collins
Chairman
The Honorable Joseph I. Lieberman
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

The Honorable Ernest F. Hollings
Ranking Minority Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Adam H. Putnam
Chairman
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
Committee on Government Reform
House of Representatives

Technology Assessment Overview

Our nation's critical infrastructures include those assets, systems, and functions vital to our national security, economic need, or national public health and safety. Critical infrastructures encompass a number of sectors, including many basic necessities of our daily lives, such as food, water, public health, emergency services, energy, transportation, information technology and telecommunications, banking and finance, and postal services and shipping. All of these critical infrastructures increasingly rely on computers and networks for their operations. Many of the infrastructures' networks are also connected to the public Internet. While the Internet has been beneficial to both public and private organizations, the critical infrastructures' increasing reliance on networked systems and the Internet has increased the risk of cyber attacks that could harm our nation's infrastructures.

Cybersecurity refers to the defense against attacks on our information technology infrastructure. Cybersecurity is a major concern of both the government and the private sector.[1] Technologies such as firewalls and antivirus software can be deployed to help secure critical infrastructures against cyber attacks in the near term, but additional research can lead to more secure systems. While there are many challenges to improving cybersecurity for critical infrastructures, there are potential actions available to infrastructure owners and the federal government. Since 1997, we have designated information security as a government-wide high-risk issue. In January 2003, we expanded this high-risk issue to emphasize the increased importance of protecting the information systems that support critical infrastructures.[2]

This technology assessment focuses on the use of cybersecurity technologies for critical infrastructure protection (CIP). Consistent with guidance provided by the Senate's Fiscal Year 2003 Legislative Branch Appropriations Report (Senate Report 107-209), we began this assessment in response to a request from the chairman and ranking minority member

[1]It is important to note that physical security and cybersecurity are intertwined and both are necessary to achieve overall security. Physical security typically involves protecting any physical asset—from entire buildings to computer hardware—from physical attacks, whereas cybersecurity usually focuses on protecting software and data from attacks that are electronic in nature and that typically arrive over a data communication link.

[2]U.S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: Jan. 2003). This report highlights our key prior findings and recommendations for federal information security and critical infrastructure protection.

of the Senate Committee on Governmental Affairs; the ranking minority member of the Senate Committee on Commerce, Science, and Transportation; and the chairman of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform. The assessment addresses the following questions:

1. What are the key cybersecurity requirements in each of the critical infrastructure protection sectors?

2. What cybersecurity technologies can be applied to critical infrastructure protection? What technologies are currently deployed or currently available but not yet widely deployed for critical infrastructure protection? What technologies are currently being researched for cybersecurity? Are there any gaps in cybersecurity technology that should be better researched and developed to address critical infrastructure protection?

3. What are the implementation issues associated with using cybersecurity technologies for critical infrastructure protection, including policy issues such as privacy and information sharing?

To answer these questions, we began by reviewing previous studies on cybersecurity and critical infrastructure protection, including those from the National Research Council, the CERT® Coordination Center (CERT/CC), the Institute for Information Infrastructure Protection (I3P), the National Institute of Standards and Technology (NIST), and GAO. We used a data collection instrument to interview representatives of several critical infrastructure sectors, as identified in national strategy documents. We met with officials from the Department of Homeland Security's (DHS) Information Analysis and Infrastructure Protection (IAIP) directorate to discuss their efforts in organizing and coordinating critical infrastructure protection activities. In addition, we met with representatives of the National Science Foundation (NSF), NIST, the National Security Agency (NSA), the Advanced Research and Development Activity, the Infosec Research Council, and DHS's Science and Technology directorate to discuss current and planned federal cybersecurity research efforts. We also met with representatives from two Department of Energy national laboratories, Sandia National Laboratories and Lawrence Livermore National Laboratory, and from Software Engineering Institute's CERT/CC. We interviewed cybersecurity researchers from academic institutions (Carnegie Mellon University, Dartmouth College, and the University of California at Berkeley) and corporate research centers (AT&T Research

Laboratories, SRI International, and HP Laboratories). Based on our initial analysis, we prepared a draft assessment outlining the cybersecurity challenges in critical infrastructure protection and actions that could be undertaken by key stakeholders. In October 2003, we convened a meeting, with the assistance of the National Academy of Sciences (NAS), to review the preliminary results of our work. Meeting attendees included representatives from academia, critical infrastructure sectors, and public policy organizations. We incorporated the feedback from the meeting attendees into the draft report. We provided our draft assessment report to DHS and NSF for their review. We also had the draft report reviewed by selected attendees of the meeting that NAS convened for this work, as well as by members of other interested organizations.

We conducted our work from May 2003 to February 2004 in the Washington, D.C., metropolitan area; the San Francisco, California, metropolitan area; Princeton, New Jersey; and Pittsburgh, Pennsylvania. We performed our work in accordance with generally accepted government auditing standards.

Our report describes the cybersecurity requirements of critical infrastructure sectors and their use of information technology. Currently available cybersecurity technologies and standards are organized by control categories. The report then covers cybersecurity implementation issues. We provide some guidance for infrastructure owners on using a risk-based framework to implement current cybersecurity technologies. We also identify specific actions that the federal government could initiate or continue, along with a policy analysis framework that could guide the implementation of these actions. Finally, in appendixes, we provide a summary of federal government's CIP policies and present technical details of current cybersecurity technologies.

Background

Since the early 1990s, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity also poses significant risks to the government's and our nation's computer systems and, more important, to the critical operations and infrastructures they support. The speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, allow unauthorized individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations, for mischievous or malicious purposes including fraud or sabotage.

CIP involves activities that enhance the security of our nation's cyber and physical public and private infrastructures that are critical to national security, national economic security, or national public health and safety. With about 85 percent of the nation's critical infrastructures owned and operated by the private sector, public-private partnership is crucial for successful critical infrastructure protection.

Recent terrorist attacks and threats have further underscored the need to manage and encourage CIP activities. Vulnerabilities are being identified on a more frequent basis, which, if exploited by identified threats, could disrupt or disable several of our nation's critical infrastructures.

Through a number of strategy and policy documents, including the recent Homeland Security Presidential Directive 7 (HSPD-7), the federal government has identified several critical infrastructure sectors (see table 1) and sector-specific agencies that are to work with the sectors to coordinate CIP activities. The critical infrastructure owners are ultimately responsible for addressing their own cybersecurity needs, but several other stakeholders play critical roles in enhancing cybersecurity for CIP. These include organizations representing sectors, such as sector coordinators and information sharing and analysis centers (ISAC), the federal government, and information technology (IT) vendors. Sector coordinators are individuals or organizations that help and encourage the entities within their sector to improve cybersecurity.

Table 1: Critical Infrastructure Sectors Defined in Federal CIP Policy

Sector	Description
Agriculture	Includes supply chains for feed and crop production.
Banking and finance	Consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions, including clearing and settlement.
Chemicals and hazardous materials	Produces more than 70,000 products essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.
Emergency services	Includes fire, rescue, emergency medical services, and law enforcement organizations.
Energy	Includes electric power and the refining, storage, and distribution of oil and natural gas.
Food	Covers the infrastructures involved in post-harvest handling of the food supply, including processing and retail sales.
Government	Ensures national security and freedom and administers key public functions.
Information technology and telecommunications	Provides information processing systems, processes, and communications systems to meet the needs of businesses and government.
Postal and shipping	Includes the U.S. Postal Service and other carriers that deliver private and commercial letters, packages, and bulk assets.
Public health and healthcare	Consists of health departments, clinics, and hospitals.
Transportation	Includes aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit that are vital to our economy, mobility, and security.
Drinking water and water treatment systems	Includes about 170,000 public water systems that rely on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.

Source: GAO analysis based on the President's national strategy documents and HSPD-7.

Results in Brief

All critical infrastructure owners rely on computers in a networked environment. Although all infrastructure sectors make use of similar computer and networking technologies, specific cybersecurity requirements in each sector depend on many factors, such as the sector's risk assessments, priorities, applicable government regulations, market forces, culture, and the state of its IT infrastructure. These factors, in combination with financial and other factors like costs and benefits, can affect an infrastructure entity's use of IT as well as its deployment of cybersecurity technologies.

Cybersecurity Technologies

There are a number of cybersecurity technologies that can be used to better protect critical infrastructures from cyber attacks, including access control technologies, system integrity technologies, cryptography, audit

and monitoring tools, and configuration management and assurance technologies. In each of these categories, many technologies are currently available, while other technologies are still being researched and developed. Table 2 summarizes some of the common cybersecurity technologies, categorized by the type of security control they help to implement.

Table 2: Common Cybersecurity Technologies

Category	Technology	What it does
Access control		
Boundary protection	Firewalls	Controls access to and from a network or computer.
	Content management	Monitors Web and messaging applications for inappropriate content, including spam, banned file types, and proprietary information.
Authentication	Biometrics	Uses human characteristics, such as fingerprints, irises, and voices to establish the identity of the user.
	Smart tokens	Establish identity of users through an integrated circuit chip in a portable device such as a smart card or time synchronized token.
Authorization	User rights and privileges	Allow or prevent access to data and systems and actions of users based on the established policies of an organization.
System integrity	Antivirus software	Provides protection against malicious code, such as viruses, worms, and Trojan horses.
	Integrity checkers	Monitor alterations to files on a system that are considered critical to the organization.
Cryptography	Digital signatures and certificates	Uses public key cryptography to provide (1) assurance that both the sender and the recipient of a message or transaction will be uniquely identified, (2) assurance that the data have not been accidentally or deliberately altered, and (3) verifiable proof of the integrity and origin of the data.
	Virtual private networks	Allow organizations or individuals in two or more physical locations to establish network connections over a shared or public network, such as the Internet, with functionality that is similar to that of a private network using cryptography.
Audit and monitoring	Intrusion detection systems	Detect inappropriate, incorrect, or anomalous activity on a network or computer system.
	Intrusion prevention systems	Build on intrusion detection systems to detect attacks on a network and take action to prevent them from being successful.
	Security event correlation tools	Monitor and document actions on network devices and analyze the actions to determine if an attack is ongoing or has occurred. Enable an organization to determine if ongoing system activities are operating according to its security policy.
	Computer forensics tools	Identify, preserve, extract, and document computer-based evidence.

Category	Technology	What it does
Configuration management and assurance	Policy enforcement Applications	Enable system administrators to engage in centralized monitoring and enforcement of an organization's security policies.
	Network management	Allow for the control and monitoring of networks, including management of faults, configurations, performance, and security.
	Continuity of operations tools	Provide a complete backup infrastructure to maintain availability in the event of an emergency or during planned maintenance.
	Scanners	Analyze computers or networks for security vulnerabilities.
	Patch management	Acquires, tests, and applies multiple patches to one or more computer systems.

Source: GAO analysis.

Critical infrastructure sectors use all of these types of cybersecurity technologies to protect their systems. However, the level of use of technologies varies across sectors and across entities within sectors.

Cybersecurity Research

Despite the availability of current cybersecurity technologies, there is a demonstrated need for new technologies. Long-term efforts are needed, such as the development of standards, research into cybersecurity vulnerabilities and technological solutions for these problems, and the transition of research results into commercially available products.

While several standards exist for cybersecurity technology in the areas of protocol security, product-level security, and operational guidelines, there is still a need to develop standards that could help guide the use of cybersecurity technologies and processes. There are several research areas being pursued by the federal government, academia, and the private sector to develop new or better cybersecurity technologies. We have identified some of the important cybersecurity research needs shown in table 3.

Table 3: Cybersecurity Research That Needs Continuing Attention

Research area	Description
Composing secure systems from insecure components	Building complex heterogeneous systems that maintain security while recovering from failures
Security for network embedded systems	Detect, understand, and respond to anomalies in large, distributed control networks that are prevalent in electricity, oil and natural gas, and water sectors.
Security metrics and evaluation	Metrics that express the costs, benefits, and impacts of security controls from multiple perspectives—economic, organizational, technical, and risk
Socioeconomic impact of security	Legal, policy, and economic implications of cybersecurity technologies and their possible uses, structure and dynamics of the cybersecurity marketplace, role of standards and best practices, implications of policies intended to direct responses to cyber attacks.
Vulnerability identification and analysis	Techniques and tools to analyze code, devices, and systems in dynamic and large-scale environments
Wireless security	Device- and protocol-level wireless security, monitoring wireless networks, and responding to distributed denial-of-service attacks in wireless networks

Source: GAO analysis.

In addition to the need for cybersecurity research that addresses existing cybersecurity threats, there is a need for long-term research that anticipates the dramatic growth in the use of computing and networks in the coming years. Some of the possible long-term research areas include tools for ensuring privacy, embedding fault-tolerance in systems, self-managing and self-healing systems, and re-architecting the Internet. Prior information technology developments have shown that more than 10 years are often required to develop basic research concepts into commercially available products.

Cybersecurity Framework

The use of an overall cybersecurity framework can assist in the selection of technologies to protect critical infrastructure against cyber attacks.

An overall cybersecurity framework includes:

(1) determining the business requirements for security;

(2) performing risk assessments;

(3) establishing a security policy;

(4) implementing a cybersecurity solution that includes people, process, and technology to mitigate identified security risks; and

(5) continuously monitoring and managing security.

Risk assessments, which are central to this framework, help organizations to determine which assets are most at risk and to identify countermeasures to mitigate those risks. Risk assessment is based on a consideration of threats and vulnerabilities that could be exploited to inflict damage.

Even with such a framework, there often are competing demands for cybersecurity investments. For example, for some companies or infrastructures, mitigating physical risks may be more important than mitigating cyber risks. Further, investing in cybersecurity technologies needs to make business sense. For some critical infrastructure owners, national security and law enforcement needs do not always outweigh the business needs of the entity. Without legal requirements for cybersecurity, security officers often need to justify cybersecurity investments using either strategic or financial measures. Further, critical infrastructures and their component entities are often dependent on systems and business functions that are beyond their control, such as other critical infrastructures and federal and third-party systems.

Several of the currently available cybersecurity technologies could, if used properly, improve the cybersecurity posture of critical infrastructures. It is important to bear in mind the limitations of some cybersecurity technologies and to be aware that their capabilities should not be overstated. Technologies do not work in isolation. Cybersecurity solutions make use of people, process, and technology. Cybersecurity technology must work within an overall security process and be used by trained personnel. In our prior reviews of federal computer systems, we found numerous instances of cybersecurity technology being poorly implemented, which reduced the effectiveness of the technology to protect

systems from attack. Best practices and guidelines are available from organizations such as NIST to assist infrastructure owners in selecting and implementing cybersecurity technologies. To increase the use of currently available cybersecurity technologies, various efforts can be undertaken. These efforts could include improving the cybersecurity awareness of computer users and administrators, considering security when developing systems, and enhancing information sharing mechanisms between the federal government and critical infrastructure sectors, state and local government, and the public.

Federal Government Actions to Improve Cybersecurity of Critical Infrastructures

Because about 85 percent of the nation's critical infrastructure is owned by the private sector, the federal government cannot by itself protect the critical infrastructures. There are three broad categories of actions that the federal government can undertake to increase the usage of cybersecurity technologies. First, the federal government can take steps to help critical infrastructures determine their cybersecurity needs, and hence their needs for cybersecurity technology. These actions include developing a national CIP plan, assisting infrastructure sectors with risk assessments, providing threat and vulnerability information to sector entities, enhancing information sharing by critical infrastructures, and promoting cybersecurity awareness. These activities can help infrastructure entities determine their needs for cybersecurity technology. This information can help the federal government to prioritize its actions and to assess the need to take further action to encourage the use of cybersecurity technology by critical infrastructure entities. Because the security needs of critical infrastructure could differ from the commercial enterprise needs of infrastructure entities, the federal government could assess the needs for grants, tax incentives, regulations, or other public policy tools to encourage nonfederal entities to acquire and implement appropriate cybersecurity technologies.

Second, the federal government can take actions to protect its own systems, including parts of the critical infrastructure. These actions could lead others to emulate the federal government or could lead to the development and availability of more cybersecurity technology products. Third, the federal government can take long-term actions to increase the quality and availability of cybersecurity technologies available in the marketplace. Table 4 highlights many of the federal policy options and some examples of the current or planned activities undertaken by the federal government that implement these options.

Table 4: Policy Options and Examples of Current or Planned Federal Activities to Improve Critical Infrastructure Cybersecurity

Policy option	Description	Examples of federal activities
Develop a national CIP plan	The plan could be used as a framework for federal CIP activities. The plan should clearly define the roles and responsibilities of federal and nonfederal CIP organizations, define objectives milestones, set time frames for achieving objectives, and establish performance measures.	According to HSPD-7, by December 2004, DHS is to produce a comprehensive and integrated plan for critical infrastructure protection that will outline national goals, objectives, milestones, and key initiatives.
Assist infrastructures with risk assessments	Provide funding to sectors and sector entities to conduct risk assessments so that vulnerabilities, threats, and mitigation strategies can be identified.	The Environmental Protection Agency (EPA) has provided funding to assist utilities for large drinking water systems in preparing vulnerability assessments. The Department of Transportation has performed a vulnerability assessment of the surface transportation sector and of the sector's reliance on the Global Positioning System. HSPD-7 directs sector-specific agencies to conduct or facilitate vulnerability assessments in each sector.
Provide threat and vulnerability information to critical infrastructures	Increase the private sector's awareness of cyber threats and the need for cybersecurity technologies by improving the federal government's capabilities to identify, analyze, and disseminate information about threats to and vulnerabilities of critical infrastructure sectors and their member entities.	DHS gathers and disseminates information on threats to critical infrastructures and issues warning products in response to increases in the threat condition.
Enhance information sharing by critical infrastructures	Increase the federal government's and the private sector's awareness of cyber threats and the effective implementation of technology by developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector.	The Department of the Treasury has contracted with the Financial Services ISAC to improve its capabilities so that it can better share information about threats and response strategies. The InfraGard program provides the Federal Bureau of Investigation with a means for sharing information securely with individual members. EPA issued a $2 million grant to the Association of Metropolitan Water Agencies to help support the on-going efforts of the Water Information Sharing and Analysis Center, a state-of-the-art, secure information system that shares up-to-date threat and incident information between the intelligence community and the water sector.
Promote cybersecurity awareness	Ensure that the private sector is aware of the cybersecurity services that are provided by the federal government and the critical infrastructure sectors.	The Federal Deposit Insurance Corporation has sponsored conferences with the financial services sector to make sector members aware of CIP-related services provided by the federal government and the private sector.

Policy option	Description	Examples of federal activities
Promote the use of cybersecurity technologies and processes	Provide tax incentives or funding to sector entities to purchase cybersecurity technology to better protect, detect, or react to cyber attacks. The government could require the use of particular cybersecurity technologies or processes. This could also be accomplished through regulations. This option requires the development of minimum standards for cybersecurity technology.	HSPD-7 instructs sector-specific agencies to encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructures.
Develop standards and guidelines	Develop protocol and product standards for cybersecurity technology and operational guidelines for the selection, implementation, and management of cybersecurity technologies. In addition, guidance could also be provided to critical infrastructure owners on how to perform risk assessments.	In response to the Federal Information Security Management Act (FISMA) of 2002, NIST is leading the development of key information system security standards and guidelines as part of its FISMA Implementation Project. NIST and NSA are using the Common Criteria to develop comprehensive security requirements and specifications for key technologies that will be used by the federal government. The Defense Information Systems Agency (DISA) and NSA have also prepared implementation guides to help system administrators to configure their systems in a secure manner.
Secure federal government systems	Implement appropriate management, operational, and technical controls to secure critical federal computer systems from cyber attacks. Critical infrastructure owners rely on federal computer systems to provide certain services.	FISMA requires federal agencies to provide risk-based information security protections for their computer systems. *The National Strategy to Secure Cyberspace* identifies the need to secure government's cyberspace as one of its five priorities.
Procure secure products and services for the federal government	Require sector entities to address cybersecurity needs prior to interacting with government computer systems. Impose security requirements in federal procurements of information technology.	*The National Strategy to Secure Cyberspace* states that the federal government is identifying ways to improve security in agency contracts and evaluating the overall procurement process as it relates to security.
Foster cooperation with foreign countries regarding cyber attacks	Because cyber attacks may not originate in the United States and could cross several geopolitical boundaries, the cooperation of foreign countries is important to facilitate the tracing of cyber attacks and the apprehension of attackers.	*The National Strategy to Secure Cyberspace* states that the United States will actively foster international cooperation in investigating and prosecuting cyber crime. HSPD-7 assigns the State Department this responsibility.
Develop cybersecurity education programs	Teach the importance of cybersecurity and how to use information technology securely. Increase the number of trained computer security professionals.	The Department of Justice has a Cyberethics for Kids program that teaches students in elementary and middle schools about the risks of some online behavior and ways to protect themselves from such behavior. NSF administers the Federal Cyber Service in universities to increase the number of cybersecurity professionals.

Policy option	Description	Examples of federal activities
Fund the research and development of cybersecurity technology	Provide funding to research and develop new technologies.	The Defense Advanced Research Projects Agency, DHS, NSF, NIST, and NSA have ongoing efforts to research and develop new cybersecurity technologies. CIP policy documents identify the further need to better prioritize and coordinate research efforts.

Source: GAO analysis.

As table 4 shows, the federal government is already taking several actions to improve the cybersecurity posture of critical infrastructure sectors. For example, it has designated sector-specific agencies for each critical infrastructure sector that are to work with their counterparts in the private sector to assess sector vulnerabilities and to develop plans to eliminate those vulnerabilities. It has helped to fund risk assessment activities in both the water and the surface transportation sectors. Through agencies such as NIST, DISA, and NSA, the federal government has published a variety of best practices and guidelines that assist in the planning, selection, and implementation of cybersecurity technologies. These guidelines could also prove useful to private sector infrastructure entities. DHS provides vulnerability and threat information to critical infrastructures. Agencies, such as the Department of Justice and NSF, have established educational programs designed to teach students about cybersecurity. The federal government has also let several grants to support cybersecurity technology research and development.

Policy Analysis Framework for Federal Actions

When deciding whether to continue or expand existing programs or to create new programs, it will be important for the federal government to consider the scope of the problem and the costs and benefits, the implementation issues, and the consequences of each option. Factual information is needed on the scope and scale of cyber vulnerabilities and the consequences of possible cyber attacks on critical infrastructures. The technology issues surrounding the problem and the structure of the security marketplace have to be determined. To help determine the proper approach for federal action, the government will require information from the private sector on the scope and size of the cybersecurity problem and the actions that the private sector is already taking to address the problem. Further, information on critical infrastructure assets, vulnerabilities, and priorities, which could be gleaned if private sector entities follow the risk-based framework for security that we have described, is needed from the private sector.

As with any federal program, it will be important to measure the results of any federal cybersecurity program. However, the lack of well-defined

security standards or benchmarks makes it difficult to measure the benefit of such a program. Further, what may be appropriate for some sectors may not be appropriate for others. While all sectors place some value on protecting the confidentiality, integrity, and availability of their computer systems and data, the relative importance of these objectives varies among the sectors. Further, because of business or other demands, the emphasis on cybersecurity issues varies from entity to entity and from sector to sector.

It is also important to consider the proper role of the federal government. Sometimes, the best course of action may be to take no action at all. In some critical infrastructure sectors, private sector responses may adequately address a problem so that federal involvement is not required. For example, according to chemical infrastructure sector officials, during the second quarter of 2003, the Chemical Industry Data Exchange (CIDX) released its cybersecurity guidance for the Responsible Care Security Code, cybersecurity guidance for security vulnerability assessment methodology, and the results of baseline assessments against the ISO 17799 standard for security management practices. The railroad sector has conducted a risk assessment that identified and evaluated threats to and vulnerabilities of the rail system, quantified the risks, and devised appropriate countermeasures.

Because many organizations are involved in this nation's critical infrastructure protection, it is important for all levels of government—federal, state, and local—and the private sector to work cooperatively to ensure that the most critical cybersecurity issues are addressed. A national CIP plan that defines the roles and responsibilities of federal and nonfederal CIP organizations; identifies and prioritizes critical assets, systems, and functions; and establishes standards and benchmarks for infrastructure protection could help the federal government to apply its limited resources where they are most needed. Ultimately, the protection of critical infrastructures in this country falls on the critical infrastructure owners. However, as we have described, the federal government has several options at its disposal to manage and encourage the increased use of cybersecurity technologies, research and develop new cybersecurity technologies, and generally improve the cybersecurity posture of critical infrastructure sectors.

Agency Comments and External Reviewer Comments

We provided a draft of this report to the Department of Homeland Security and the National Science Foundation for their review. DHS generally concurred with the report and provided detailed comments, which we incorporated as appropriate. NSF said that this is an important and timely

report that provides broad coverage of current and emerging cybersecurity and infrastructure technologies. We include DHS's and NSF's comments in appendixes IV and V, respectively, and summarize them in chapter 5.

We also provided a draft of this report to 26 organizations, representing government, industry, and academia, for their review. We received comments and suggestions from 15 reviewers. The comments included the clarification of issues and the highlighting of certain aspects of the assessment that reviewers considered important. We have incorporated these comments, where appropriate, in the report. We summarize these comments in chapter 5.

Chapter 1: Introduction

Computers have been crucial to the operations of government and business. In the early days of computing, computers calculated the designs of the first strategic weapons and projections of bombing effectiveness. Businesses used computers to automate business calculations. The role of computers evolved into record keeping and automating many tasks to the point that, by now, computers play a role in nearly everything. The advent of networking made it possible for computers to communicate and become even more pervasive. Nowadays, our water, food, fuel, lights, heat, home, work, and vehicles are all supported, if not directly run, by computers and networks. Essentially, computers and networks run our nation's critical infrastructures that are vital to national defense, economic security, and public health and safety.

Unfortunately, many computer systems and networks were not designed with security in mind. As a result, the core of our critical infrastructure is riddled with vulnerabilities that seem to require constant patches and fixes. These vulnerabilities could enable an attacker to disrupt the operations of or cause damage to critical infrastructures. The potential exists for causing physical damage to people and property by exploiting vulnerabilities in computers and networks. The problem is exacerbated by increasing computer interconnectivity, most notably growth in the use of the Internet since the 1990s. While the benefits of the Internet have been enormous, widespread interconnectivity also poses enormous risks to computer systems and to the critical operations and infrastructures they support. Reliance on the Internet has created a new avenue for attack on infrastructures. These attacks are called *cyber attacks* because they arrive over the network by means of information packets that traverse communication links and attack cyber assets—the software and data. We have seen these cyber attacks in the form of viruses and worms—malicious software that is designed to propagate from one system to another, either automatically or by some user action such as opening an e-mail attachment. Because of the increasing threats of cyber attacks, *cybersecurity*—the defense against cyber attacks—is a major concern of the government and the private sector.

There is a variety of technologies that can be used in support of cybersecurity. Some technologies, such as firewalls and biometrics, help to protect computers and networks against attacks, while others, such as intrusion detection systems and continuity of operations tools, help to detect and respond to cyber attacks in progress.

Critical infrastructure protection (CIP) involves activities that enhance the security of our nation's cyber and physical public and private

infrastructure that are critical to national security, national economic security, or national public health and safety. Federal awareness of the importance of securing our nation's critical infrastructures has continued to evolve since the mid-1990s. Recent terrorist attacks and threats have further underscored the need to manage and encourage CIP activities. Numerous vulnerabilities are being identified more and more frequently which, if exploited by the increasing number of threats, could disrupt or disable several of our nation's critical infrastructures. However, with about 85 percent of the nation's critical infrastructures owned and operated by the private sector, CIP is not an endeavor that the federal government can undertake alone. Since 1997, we have designated information security as a government-wide high-risk issue.[1] In January 2003, we expanded this high-risk issue to emphasize the increased importance of protecting the information systems that support critical infrastructures.[2]

Critical Infrastructure Protection Policy Has Evolved since the Mid-1990's

Since the mid-1990s, the federal government has articulated its approach to CIP through several reports, orders, directives, laws, and strategy documents. Appendix II describes the policies in more detail. Within the federal government, the Department of Homeland Security (DHS) has a number of responsibilities for critical infrastructure protection, including the responsibility to (1) develop a comprehensive national CIP plan; (2) recommend CIP measures in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities; and (3) disseminate, as appropriate, information analyzed by the department both within DHS and to other federal agencies, state and local government agencies, and private sector entities. Within DHS, the Information Analysis and Infrastructure Protection (IAIP) directorate serves as the primary point of contact for CIP activities. Most recently, Homeland Security Presidential Directive 7 (HSPD-7) established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources and to protect them from terrorist attack. To ensure the coverage of critical sectors, HSPD-7 designates sector-specific agencies for the critical

[1]This series identifies areas at high risk because of either their greater vulnerabilities to waste, fraud, abuse, and mismanagement or major challenges associated with their economy, efficiency, or effectiveness.

[2]U.S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: Jan. 2003).

infrastructure sectors identified in the *National Strategy for Homeland Security* (see table 5).

Table 5: Critical Infrastructure Sectors Identified by the Federal Government

Sector	Description	Sector-specific agencies
Agriculture	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production.	Department of Agriculture
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions including clearing and settlement.	Department of the Treasury
Chemicals and hazardous materials	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical industry represents a $450 billion enterprise and produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction and other necessities.	Department of Homeland Security
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Emergency services	Saves lives and propertyfrom accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	Department of Homeland Security
Energy	Provides the electric power used by all sectors, including critical infrastructures, and the refining, storage, and distribution of oil and natural gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Food	Carries out the post-harvesting of the food supply, including processing and retail sales.	Department of Agriculture and Department of Health and Human Services
Government	Ensures national security and freedom and administers key public functions.	Department of Homeland Security
Information technology and telecommunications	Provides communications and processes to meet the needs of businesses and government.	Department of Homeland Security
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector.	Department of Homeland Security
Public health and healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Transportation	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	Department of Homeland Security
Drinking water and water treatment systems	Sanitizes the water supply with the use of about 170,000 public water systems. These systems depend on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.	Environmental Protection Agency

Source: GAO analysis based on the President's national strategy documents and HSPD-7.

Sector-specific agencies are responsible for infrastructure protection activities in their assigned sectors and are to coordinate and collaborate with relevant federal agencies, state and local governments, and the private sector to accomplish these responsibilities. To facilitate private sector participation, federal CIP policy states that sector-specific agencies are to support sector-coordinating mechanisms. In addition, the federal government's CIP approach encourages the voluntary creation of information sharing and analysis centers (ISAC) that facilitate gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through DHS.

Federal and Private Sector Computer Security Is Affected by Various Laws

Several laws affect the cybersecurity of federal and private sector entities and could drive the development of cybersecurity-related tools. These laws include requirements for federal agency information security programs, funding for security research and grant programs, and requirements for private sector entities to protect citizens' personal, financial, and medical information. For example, the Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to provide risk-based information security protections for information collected or maintained by or on behalf of an agency, as well as information systems used or operated by an agency or by a contractor or other organization on behalf of an agency.[3] According to FISMA, agencies are to identify and provide information security protection commensurate with the risk and magnitude of the potential harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 required the electronic exchange of information and mandated protections for the privacy and security of this information.[4] In 1999, the Gramm-Leach-Bliley Act established a new requirement for protecting the privacy of personal financial information.[5] In the area of research funding, the Cyber Security Research and Development Act authorized funding for computer and network security

[3]Federal Information Security Management Act of 2002, Title III, Public Law 107-347 (Dec. 17, 2002).

[4]Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (Aug. 21, 1996).

[5]Gramm-Leach-Bliley Act of 1999, Public Law 106-102 (Nov. 12, 1999).

research and grant programs through NIST and the National Science Foundation (NSF).[6]

Report Overview

This technology assessment focuses on three key questions:

1. What are the key cybersecurity requirements in each of the critical infrastructure protection sectors?

2. What cybersecurity technologies can be applied to critical infrastructure protection? What technologies are currently deployed or currently available but not yet widely deployed for critical infrastructure protection? What technologies are currently being researched for cybersecurity? Are there any gaps in cybersecurity technology that should be better researched and developed to address critical infrastructure protection?

3. What are the implementation issues associated with using cybersecurity technologies for critical infrastructure protection, including policy issues such as privacy and information sharing?

To answer these questions, we describe the critical infrastructure sectors, the efforts currently being taken to improve their cybersecurity postures, and the challenges they face in implementing cybersecurity strategies. While critical infrastructure protection must guard against both physical and cyber threats, we focus our report on approaches to protect against cyber threats. We describe how several cybersecurity technologies work and how they can be applied to cybersecurity problems. We discuss the limitations to some of these technologies. We also describe ongoing cybersecurity research and some of the key areas that require further work. We identify challenges to improving cybersecurity and several options available to the federal government to improve the cybersecurity posture of critical infrastructure sectors.

[6]The Cyber Security Research and Development Act of 2002, Public Law 107-305 (Nov. 27, 2002).

Chapter 2: Cybersecurity Requirements of Critical Infrastructure Sectors

Protecting our nation's critical infrastructures is a formidable challenge. Numerous threats and vulnerabilities are being identified on a more frequent basis. If these vulnerabilities can be successfully exploited by threats, several of our nation's critical infrastructures could be disrupted or disabled. To assess the need for cybersecurity technology, it is important to understand the cybersecurity needs of critical infrastructure sectors by examining the threats that they face as well as the vulnerabilities that could be exploited. Further, to determine the information technology (IT) assets that will need to be protected, it is important to examine the types of computer and networking technologies that are used in various sectors.

Threats, Vulnerabilities, Incidents, and the Consequences of Potential Attacks Are Increasing

Critical infrastructures can be threatened using both physical and cyber means. Several organizations and individuals are capable of conducting such attacks. Historically, attacks on our infrastructures could be conducted only by a relatively small number of entities. However, with critical infrastructures' increasing reliance on computers and networks, more organizations and individuals can cause harm using cyber attacks. Further, U.S. authorities are becoming increasingly concerned about the prospect of combined physical and cyber attacks that could have devastating consequences. Table 6 lists sources of threats that have been identified by the U.S. intelligence community.

Table 6: Threats to Critical Infrastructure

Threat	Description
Criminal groups	International corporate spies and organized crime organizations pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency (CIA), the large majority of hackers do not have the requisite tradecraft to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message. Most international hacktivist groups appear bent on propaganda rather than damage to critical infrastructures.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
National governments and foreign intelligence services	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. citizens across the country. The threat from national cyber warfare programs is unique because they pose a threat along the entire spectrum of objectives that might harm U.S. interests. According to the CIA, only government-sponsored programs are developing capabilities with the prospect of causing widespread, long-duration damage to U.S. critical infrastructures.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States are less developed in their computer network capabilities than other adversaries. Terrorists likely pose a limited cyber threat. The CIA believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.

Source: GAO analysis based on data from the FBI, CIA, and CERT/CC.

Over the last decade, physical and cyber events, as well as related analyses by various organizations, have demonstrated the increasing threats faced by critical infrastructure sectors in the United States. For example, on February 11, 2003, the National Infrastructure Protection Center (NIPC)

issued an advisory to heighten the awareness of an increase in global hacking activities as a result of the increasing tensions between the United States and Iraq. This advisory noted that during a time of increased international tension, illegal cyber activity often escalates, such as spamming, Web page defacements, and denial-of-service attacks. Further, this activity can originate within another country that is party to the tension, can be state sponsored or encouraged, or can come from domestic organizations or individuals independently. The advisory also stated that attacks may have one of several objectives, including political activism targeting Iraq or those sympathetic to Iraq by self-described "patriot" hackers, political activism or disruptive attacks targeting U.S. systems by those opposed to any potential conflict with Iraq, or even criminal activity masquerading or using the current crisis to further personal goals.

Respondents to the 2003 Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) Computer Crime and Security Survey identified independent hackers as the most likely source of cyber attacks, as shown in table 7.[1]

Table 7: Likely Sources of Cyber Attacks According to Respondents to the CSI/FBI 2003 Computer Crime and Security Survey

Potential source	Percentage of respondents
Independent hackers	82%
Disgruntled employees	77%
U.S. competitors	40%
Foreign governments	28%
Foreign corporations	25%

Source: 2003 CSI/FBI Computer Crime and Security Survey.

It is important to consider the threat posed by insiders. According to the CSI/FBI survey, 45 percent of respondents reported unauthorized access by insiders, and 80 percent of respondents reported insider abuses of network access. As shown in table 7, disgruntled employees are believed to be a likely source of attack by 77 percent of respondents. According to a National Security Telecommunications and Information Systems Security Committee report, insiders include employees, contractors, service

[1]Computer Security Institute, *2003 CSI/FBI Computer Crime and Security Survey* (2003).

providers, and anyone else with legitimate access to a system.[2] Insiders may have a variety of motives for their actions. For example, insiders may have views that conflict with those of the organization they are employed by and may want to impose their beliefs on the organization. Another group of insiders may just be curious and attempt to access systems they are not authorized to use. Other insiders are employees who do not intend to cause any harm to the organization but who unwittingly can cause damage either through their ignorance, carelessness, or disregard for organizational policies. Actions such as disabling antivirus software, leaving passwords on workstations, and installing unauthorized software may open a large enough vulnerability for a hacker to gain access to a system.

As larger amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available IT, the likelihood increases that information attacks will threaten vital national interests.

Critical Infrastructure Sectors Face Various Physical Threats

With the coordinated terrorist attacks against the World Trade Center, in New York City, and the Pentagon, in Washington, D.C., on September 11, 2001, the threat of terrorism rose to the top of the country's national security and law enforcement agendas. Even before these catastrophic incidents, attacks against people, property, and infrastructures had increased concerns about terrorism. The terrorist bombings in 1993 of the World Trade Center in New York City and in 1995 of the Alfred P. Murrah Federal Building in Oklahoma City prompted increased emphasis on the need to strengthen and coordinate the federal government's ability to effectively combat terrorism domestically. The 1995 Aum Shinrikyo sarin nerve agent attack in the Tokyo subway system also raised new concerns about U.S. preparedness to combat terrorist incidents involving weapons of mass destruction.[3] However, as clearly demonstrated by the September 11, 2001 incidents, a terrorist attack would not have to fit the definition of weapons of mass destruction to result in mass casualties, destruction of

[2]National Security Telecommunications and Information Systems Security Committee, *The Insider Threat to U.S. Government Information Systems*, NSTISSAM INFOSEC/1-99 (Fort Meade, MD: July 1999). In 2001, this committee was redesignated the Committee on National Security Systems.

[3]A weapon of mass destruction is a chemical, biological, radiological, or nuclear agent or weapon.

critical infrastructures, economic losses, and disruption of daily life nationwide.

U.S. intelligence and law enforcement communities continuously assess both foreign and domestic terrorist threats to the United States. The U.S. foreign intelligence community—for example, the CIA, the Defense Intelligence Agency, the FBI, and the Department of State's Bureau of Intelligence and Research—monitors terrorist threats of foreign origin. In addition, the FBI gathers intelligence and assesses the threat posed by domestic sources. According to the U.S. intelligence community, conventional explosives and firearms continue to be terrorists' weapons of choice. The community also believes that terrorists are less likely to use weapons of mass destruction, although the possibility that they will use these weapons may increase over the next decade. Table 8 identifies weapons that can be used to physically attack critical infrastructure.

Table 8: Weapons for Physically Attacking Critical Infrastructures

Weapon	Description
Biological weapons	Biological weapons, which release large quantities of living, disease-causing microorganisms, have extraordinary lethal potential. Biological weapons are relatively easy to manufacture, requiring straightforward technical skills, basic equipment, and a seed stock of pathogenic microorganisms. Biological weapons are especially dangerous because we may not know immediately that we have been attacked, allowing an infectious agent time to spread. Moreover, biological agents can serve as a means of attack against humans as well as livestock and crops, inflicting casualties as well as economic damage.
Chemical weapons	Chemical weapons are extremely lethal and capable of producing tens of thousands of casualties. Like biological weapons, chemical weapons are relatively easy to manufacture, using basic equipment, trained personnel, and precursor materials that often have legitimate dual uses. As the 1995 Tokyo subway attack revealed, even sophisticated nerve agents are within the reach of terrorist groups.
Nuclear weapons	Nuclear weapons have enormous destructive potential. Terrorists who seek to develop a nuclear weapon must overcome two formidable challenges. First, acquiring or refining a sufficient quantity of fissile material is very difficult—though not impossible. Second, manufacturing a workable weapon requires a very high degree of technical capability—though terrorists could feasibly assemble the simplest type of nuclear device. To get around these significant though not insurmountable challenges, terrorists could seek to steal or purchase a nuclear weapon.
Radiological weapons	Radiological weapons, or "dirty bombs," combine radioactive material with conventional explosives. The individuals and groups engaged in terrorist activity can cause widespread disruption and fear, particularly in heavily populated areas.
Conventional means	Terrorists, both domestic and international, continue to use traditional methods of violence and destructionto inflict harm and spread fear. They have used knives, guns, and bombs to kill the innocent. They have taken hostages and spread propaganda. Given the low expense, ready availability of materials, and relatively high chance for successful execution, terrorists will continue to make use of conventional attacks.

Source: *National Strategy for Homeland Security.*

Nevertheless, in February 2004, the Director of Central Intelligence testified that in his view, terrorist organizations continue to pursue chemical, biological, radiological, and nuclear weapons.[4] He also stated that although the Al Qaeda leadership is seriously damaged, it, along with other groups supporting its views, continues to pose a threat to the United States. In addition, he stated that terrorism directed at U.S. interests goes beyond religious extremist groups, adding that the Revolutionary Armed Forces of Colombia and the Revolutionary People's Liberation Party/Front—a Turkish group—have shown a willingness to attack U.S. targets.

Critical Infrastructure Sectors Face Various Cyber Threats

In addition to posing these physical threats, terrorists and others with malicious intent, such as transnational criminals and foreign intelligence services, pose a threat to our nation's computer systems. Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the National Security Agency (NSA), foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. Since the terrorist attacks of September 11, 2001, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, in February 2002, the threat to these infrastructures was highlighted by the Special Advisor to the President for Cyberspace Security, during a Senate hearing, when he stated that although to date none of the traditional terrorists groups, such as al Qaeda, had used the Internet to launch a known assault on an American infrastructure, information on water systems was discovered on computers found in al Qaeda camps in Afghanistan.[5] Also, in February 2002, the Director of Central Intelligence testified before the Senate Select Committee on Intelligence on the possibility of cyber warfare attacks by terrorists.[6] He stated that the September 11 attacks demonstrated the

[4]Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence (Feb. 24, 2004).

[5]Testimony of Richard A. Clarke, Special Advisor to the President for Cyberspace Security and Chairman of the President's Critical Infrastructure Protection Board, before the Senate Committee on the Judiciary, Subcommittee on Administrative Oversight and the Courts (Feb. 13, 2002).

[6]Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence (Feb. 6, 2002).

nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them.

According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping programs ("sniffers") that can destroy, intercept, degrade the integrity of, or deny access to data (see table 9).

Table 9: Types of Cyber Attacks

Type of attack	Description
Denial of service	A method of attack that denies system access to legitimate users without actually having to compromise the targeted system. From a single source, the attack overwhelms the target computer with messages and blocks legitimate traffic. It can prevent one system from being able to exchange data with other systems or prevent the system from using the Internet.
Distributed denial of service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bombs	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate.
War-dialing	Simple programs that dial consecutive phone numbers looking for modems.
War-driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adaptor that involves patrolling locations to gain unauthorized access.
Worms	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

Source: GAO analysis.

Viruses and worms are commonly used to launch denial-of-service attacks, which generally flood targeted networks and systems with so much transmission of data that regular traffic is either slowed or completely interrupted. Such attacks have been utilized ever since the groundbreaking

Morris worm, which brought 10 percent of the systems connected to the Internet to a halt in November 1988. In 2001, the Code Red worm used a denial-of-service attack to affect millions of computer users by shutting down Web sites, slowing Internet service, and disrupting business and government operations.

In the case of insider attacks, the use of these tools may not even be necessary because of the unfettered access insiders often have to their computer systems. An example of an insider causing damage to a system occurred at the U.S. Coast Guard in July 1997. A former U.S. Coast Guard employee used her programming skills to access the service's nationwide personnel database and deleted crucial data that caused the computer system to crash. The crash wiped out almost two weeks' worth of personnel data used to determine promotions, transfers, assignments, and disability claim reviews. It took 115 Coast Guard employees working more than 1,800 hours to recover and re-enter the data, at a cost of more than $40,000.

The growing number of known vulnerabilities increases the number of potential attacks that can be created by the hacker community. As vulnerabilities are discovered, attackers may attempt to exploit them. Attacks can be launched against specific targets or widely distributed through viruses and worms. The risks posed by this increasing and evolving threat are demonstrated in reports of actual and potential attacks and disruptions. For example,

- On August 11, 2003, the Blaster worm was launched, and it infected more than 120,000 computers in its first 36 hours. When the worm was successfully executed, it could cause the operating system to crash. The worm affected a wide range of systems and caused slowness and disruptions in users' Internet services. The worm was programmed to launch a denial-of-service attack against Microsoft's Windows Update Web site. The Maryland Motor Vehicle Administration was forced to shut down its computer systems, and systems in both national and international areas were also affected.

- According to a preliminary study coordinated by the Cooperative Association for Internet Data Analysis, on January 25, 2003, the SQL Slammer worm (also known as "Sapphire") infected more than 90 percent of vulnerable computers worldwide within 10 minutes of its release on the Internet. As the study reports, exploiting a known vulnerability for which a patch had been available since July 2002, Slammer doubled in size every 8.5 seconds and achieved its full

scanning rate (55 million scans per second) after about 3 minutes. It caused considerable harm through network outages and such unforeseen consequences as canceled airline flights and automated teller machine failures. Further, the study emphasizes that the effects would likely have been more severe had Slammer carried a malicious payload, exploited a more widespread vulnerability, or targeted a more popular service.

- In November 2002, a British computer administrator was indicted on charges that he accessed and damaged 98 computers in 14 states between March 2001 and March 2002, causing some $900,000 in damage to the computers. These networks belonged to the Department of Defense (DoD), the National Aeronautics and Space Administration, and private companies. The indictment alleges that the attacker was able to gain administrative privileges on military computers and copy password files and delete critical system files. The attacks rendered the networks of the Earle Naval Weapons Station in New Jersey and the Military District of Washington inoperable.

- On October 21, 2002, NIPC reported that all 13 root-name servers that provide the primary road map for almost all Internet communications were targeted in a massive distributed denial-of-service attack. Seven of the servers failed to respond to legitimate network traffic, and two others failed intermittently during the attack. Because of safeguards, most Internet users experienced no slowdowns or outages.

- In August 2001, we reported to a subcommittee of the House Government Reform Committee that the attacks referred to as Code Red, Code Red II, and SirCam affected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations.[7] Then, in September 2001, the Nimda worm appeared, using some of the most significant attack profile aspects of Code Red II and 1999's infamous Melissa virus, which allowed it to spread widely in a short amount of time. Security experts estimate that Code Red, Sircam, and Nimda have caused billions of dollars in damage.

As the number of individuals with computer skills has increased, more intrusion, or hacking, tools have become readily available and relatively

[7]U.S. General Accounting Office, *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures*; GAO-01-1073T (Washington, D.C.: Aug. 29, 2001).

easy to use. Frequently, skilled hackers develop exploitation tools and post them on Internet hacking sites. These tools are then readily available for others to download, allowing even inexperienced programmers to create a computer virus or to literally point and click to launch an attack. According to the National Institute of Standards and Technology (NIST), 30 to 40 new attack tools are posted on the Internet every month.[8] Experts also agree that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities that have been discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

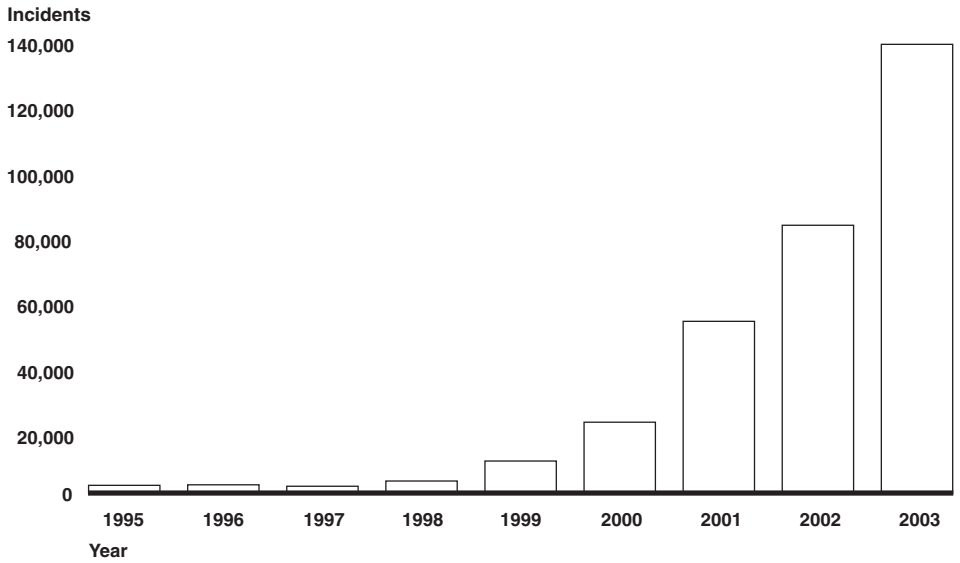
Because automated tools now exist, the CERT® Coordination Center (CERT/CC) has noted that attacks that once took weeks or months to propagate over the Internet now take just hours, or even minutes.[9] For instance, while in July 2001, Code Red achieved an infection rate of over 20,000 systems within 10 minutes, less than a year and a half later, in January 2003, the Slammer worm successfully attacked at least 75,000 systems, infecting more than 90 percent of vulnerable systems within 10 minutes.

The threat to systems connected to the Internet is illustrated by the increasing number of computer security incidents reported to CERT/CC. This number rose from just under 10,000 in 1999 to over 52,000 in 2001, to about 82,000 in 2002, and to 137,529 in 2003 (see figure 1). However, the Director of CERT Centers stated that he estimates that as much as 80 percent of actual security incidents go unreported, in most cases because (1) the organization was unable to recognize that its systems had been penetrated or there were no indications of penetration or attack, or (2) the organization was reluctant to report.

[8]U.S. General Accounting Office, *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*, GAO-01-751 (Washington D.C.: Aug. 13, 2001).

[9]The CERT/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Figure 1: Information Security Incidents, 1995-2003



Source: GAO analysis based on CERT/CC data.

In addition, flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to the growth in software flaws. For example, Microsoft Windows 2000 reportedly contains about 35 million lines of code, compared with about 15 million lines for Windows 95. As reported by NIST, based on various studies of code inspections, most estimates suggest that there are as many as 20 flaws per thousand lines of software code. While most flaws do not create security vulnerabilities,[10] the potential for these errors reflects the difficulty and complexity involved in delivering trustworthy code.[11] By exploiting software vulnerabilities, hackers and others who spread malicious code can cause significant damage, ranging from Web site defacement to taking control of entire systems, and thereby being able to read, modify, or delete sensitive

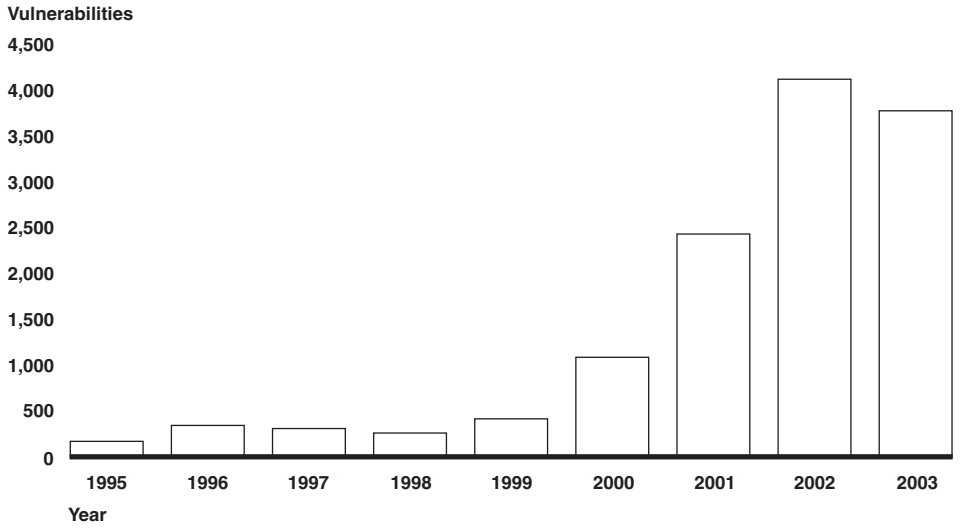
[10]A vulnerability is the existence of a flaw or weakness in hardware or software that can be exploited resulting in a violation of an implicit or explicit security policy.

[11]National Institute for Standards and Technology, *Procedures for Handling Security Patches: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-40 (Gaithersburg, MD: August 2002).

information, destroy systems, disrupt operations, or launch attacks against other organizations' systems.

Between 1995 and 2003, CERT/CC reported 12,946 security vulnerabilities that resulted from software flaws. Figure 2 illustrates the dramatic growth in security vulnerabilities over these years.

Figure 2: Security Vulnerabilities, 1995-2003



Source: GAO analysis based on CERT/CC data.

Poor Systems Management Can Be Costly and Disruptive

Despite the heightened national security and terrorism concerns occasioned by the September 11, 2001 attacks, it is important to recognize that up to the present, many of the most costly and disruptive cyber events have not been caused by malicious cyber attacks, but instead originated with mundane problems or routine systems mismanagement. For example, according to ICF Consulting, the cost to the U.S. economy of the August 14, 2003, blackout has been estimated at between $7 billion and $10 billion dollars. A joint U.S.-Canada Power System Outage Task Force investigated the causes of the blackout and issued a report in April 2004.[12] This report details a chain of mishaps, starting with a malfunctioning monitoring and

[12]U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* (Apr. 2004).

control system that was deployed by power grid operators in Ohio. Environmental factors combined with a higher than normal demand for power caused a local overload of a type that might normally trigger a brownout or a brief local blackout. System designers had not anticipated such a contingency because it involved a series of seemingly unlikely events. But what is unlikely in small systems may not be so rare in large systems. In this case, interconnectedness of the power grid permitted the disruption to spread to other operators in Canada, New York, and elsewhere on the U.S. East Coast, who could not take remedial actions because of their inability to understand what was happening.

This single event illustrates many hallmarks of what could be called the mundane cybersecurity threat:

- inadequate system monitoring and control tools;
- unplanned growth of a large, complex, system with external interdependencies;
- a combination of seemingly unlikely external factors;
- lack of a well-defined stakeholder responsible for overall robustness; and
- operator confusion and mistakes.

Mundane cybersecurity threats receive little attention, and yet are emerging as a serious risk to national economic growth and to the success of several government and private sector initiatives. These activities place computer-operated systems into critical roles for the economy, the government, the military, or nationally important industry sectors. The systems are growing through an unplanned, organic process of accretion, without any sort of global plan, and without a well-defined entity with clear responsibility for security and reliability. The resulting systems are intrinsically hard to analyze or monitor, so that even if the nation were to mandate that they be controlled, the science for doing so would often be lacking.

To make matters worse, today's mundane cybersecurity threat may become tomorrow's terrorist target. In the wake of the August 2003 blackout, many experts pointed out that even if terrorism had no role in that particular incident, terrorists could easily target the power grid with similarly spectacular results at some future time. Actions taken over an

extended period to harden nationally critical infrastructure sectors against mundane failures may thus be the best preventive measures against some future terrorist threat targeting those infrastructures. The August 2003 blackout occurred despite more than a decade of government concern about the growing risk of such instability and despite the existence of all sorts of power industry groups with responsibility for aspects of power security. The U.S.-Canada Power System Outage Task Force report reveals that while such organizations have a valuable role, with the emergence of an increasingly interconnected power grid, a need has emerged for a new kind of stakeholder with responsibility for large-scale stability of the grid.

Growing Concern over Connections between Cyber and Physical Worlds

Since September 11, 2001, the critical link between cyberspace and physical space has been increasingly recognized. As we have described, critical infrastructures face an increasing threat of cyber attacks in addition to physical attacks. In July 2002, NIPC reported that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to our critical infrastructures. As NIPC reported, the effects of a swarming attack include slowing or complicating the response to a physical attack. For instance, a cyber attack that disabled the water supply or the electrical system, in conjunction with a physical attack, could deny emergency services the necessary resources to manage the consequences of the physical attack—such as controlling fires, coordinating actions, and generating light.

Second, there is a general consensus—and increasing concern—among government officials and experts on control systems about potential cyber threats to the control systems that govern our critical infrastructures. In his November 2002 congressional testimony, the Director of the CERT Centers at Carnegie Mellon University noted that supervisory control and data acquisition (SCADA) systems and other forms of networked computer systems have been used for years to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical systems.[13] These control systems are increasingly being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions as well as to enhance performance. These computer-

[13]Testimony of Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations (Nov. 19, 2002).

controlled and network-connected systems are potential targets for individuals intent on causing massive disruption and physical damage. The use of commercial off-the-shelf technologies for these systems without adequate security enhancements can significantly limit available approaches to protection and may increase the number of potential attackers. As components of control systems increasingly make critical decisions that were once made by humans, the potential effect of a cyber attack becomes more devastating.

According to NIST, cyber attacks on energy production and distribution systems—including electric, oil, gas, and water treatment systems, as well as on chemical plants containing potentially hazardous substances—could endanger public health and safety, damage the environment, and have serious financial implications, such as loss of production, generation, or distribution of public utilities; compromise of proprietary information; or liability issues. When backups for damaged components are not readily available (e.g., extra-high-voltage transformers for the electric power grid), such damage could have a long-lasting effect.

Additionally, control system researchers at the Department of Energy's national laboratories have developed systems that demonstrate the feasibility of a cyber attack on a control system at an electric power substation, where high-voltage electricity is transformed for local use. Using tools that are readily available on the Internet, the researchers are able to modify output data from field sensors and take control of programmable logic controllers directly in order to change settings and create new output. These techniques could enable a hacker to cause an outage, thus incapacitating the substation.

Critical Infrastructures Rely on Information Technology to Operate

Entities within each of the critical infrastructure sectors rely on similar types of information technology to perform both critical and non-critical functions such as accounting, finance, personnel, manufacturing, engineering, and logistics that are essential to fulfilling their missions, such as generating and transmitting electric power, providing water, making chemicals, transporting goods and people, or supporting financial transactions.

Commercially Available Information Technologies Are Widely Deployed

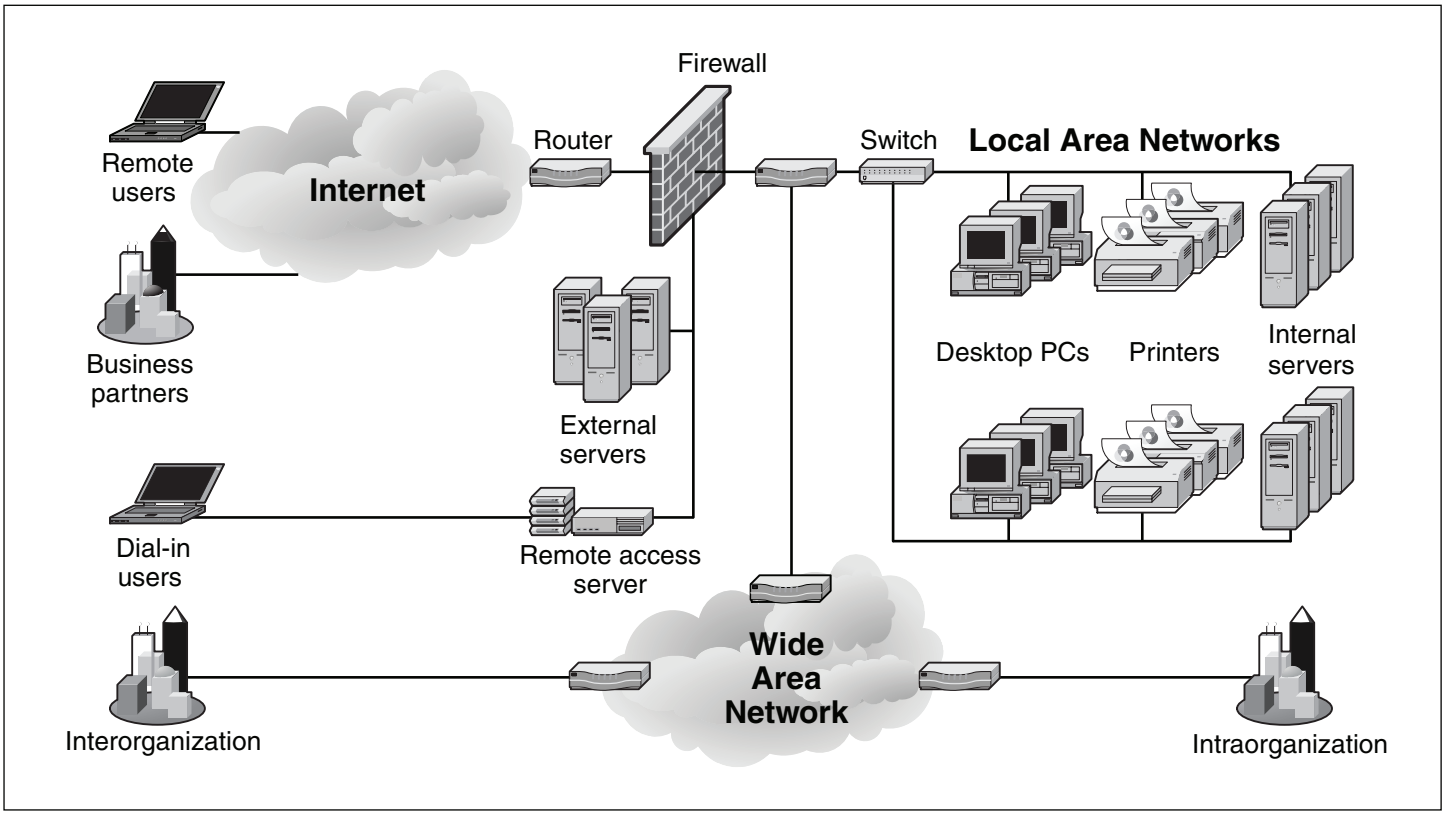
Although some critical infrastructures use proprietary systems to fulfill their missions, commercially available off-the-shelf hardware and software are commonly used across all sectors. Infrastructure sectors use both dedicated, private communication links (for example, leased fiber optics) as well as shared, public communications (such as public switched

networks and the Internet), as well as radio and satellite. These products are typically used in a networked environment to allow groups of individuals to share data, printers, communications systems, electronic mail, and other resources. These resources are provided by servers, which are computers that run specialized software to provide access to a resource or a part of the network. The network communication links between servers and devices such as printers and modems can be wired or wireless (using radio waves).

For the purposes of this assessment, we define a *network* as an interconnected collection of computers and networks. A network in a relatively small geographical area is known as a local area network (LAN). Most entities have one or more LANs at each of their offices; a LAN can be as small as two networked PCs, or it may support hundreds of users and multiple servers. Larger entities also have wide area networks (WAN) that connect the various LANs the organization has that are dispersed over a wide geographical location. Devices such as bridges, routers, and switches move *packets* (blocks of data packaged with the information necessary for their delivery) within and between networks, offering different levels of data-handling capability, depending on the origin and destination of the packets. Networks use predefined sets of rules known as *protocols* to communicate with each other. For example, the Transmission Control Protocol/Internet Protocol (TCP/IP) suite is the set of protocols used to communicate over the Internet.[14] In a TCP/IP network, each server or hardware device is assigned an IP address—a unique numeric location based on the IP addressing scheme. Every computer or device with an IP address is considered a connection point, or *node*, of the network. Each node can run network services such as the World Wide Web, electronic mail, and file transfer, storage, and retrieval. Each network service uses specific protocols and is identified by a port number that enables other nodes to locate and connect to the service. As seen in figure 3, computer servers and devices are interconnected into networks, which in turn are often connected to the Internet.

[14]The Internet refers to the specific interconnected global network of TCP/IP-based systems that began with the Department of Defense's network known as ARPANET.

Figure 3: An Example of Typical Networked Systems



Source: GAO analysis and Microsoft Visio.

Internet services and their underlying network protocols are used in the operation of infrastructures such as electric power, transportation, banking, and many more. According to infrastructure sector representatives, entities within their infrastructures use IP- and non-IP-based networks, LANs, WANs, the Internet, and other information technology. Entities also utilize a variety of operating systems and off-the-shelf and proprietary applications. In addition, they use a variety of communications methods, including satellites, radio, the public switched network, leased lines, private fiber optics, and wireless networks. Sector representatives reported the following:

- The banking and finance sector entities use all forms of information technology—client/server, Internet and non-Internet connected, proprietary, and mainframe networks. The sector's communications

are split between private (dedicated, leased, and private fiber optics) and public (public switched network, Internet). According to an industry representative, the banking and finance infrastructure sector cannot operate in the absence of information technology. The criticality of a function depends on the business context—in one context, ATMs and online banking (bill payments) are critical to customers; in another, wholesale operations are important to support infrastructure operations such as payroll and personnel. As we discuss later, the most critical systems are not controlled by the individual financial institutions but are centrally controlled by government and other entities.

- The chemical sector entities use LANs, WANs, the Internet, other IP-based networks, wireless networks, and other (non-IP-based) proprietary networks. According to industry representatives, the business processes that are most critical to sector performance are manufacturing and engineering, environmental, health and safety, supply chain and logistics, financial, and personnel.

- The defense industrial base sector uses all types of information technology to perform business functions (accounting, finance, payroll) and operational functions that could instantly affect national security operations. Two critical areas that rely on information technology are the supply chain for manufacturing and the IT infrastructure that is owned and operated by the defense industrial base for DoD.

- Within the energy sector, the electricity industry uses a combination of information technologies, including LAN, WAN, Internet, wireless networks, satellite, and radio. According to industry representatives, information technology is used for a variety of business functions and operational processes, including control functions and marketing of power to consumers. Some of these processes, such as payroll, are important to the entities but not necessarily essential from a CIP perspective.

- Also within the energy sector, the oil and natural gas industry uses a combination of information technologies, including LAN, WAN, Internet, virtual private networks, wireless networks, satellite, and radio. In addition, representatives stated that in the pipeline environment, 80 to 90 percent of the applications purchased from vendors are TCP/IP, UNIX, or Windows NT-based. The remainder are based on older or proprietary protocols, such as SNA, DECnet, Appletalk, and IPX. The sector is also reliant on specialized control

systems. The sector is highly dependent on technology for its communications and operations.

- Within the transportation sector, the rail segment relies on information technology and modern communications for rail operations and customer service. Business systems are isolated, physically separated from the control and dispatching centers. The control and dispatching systems[15] are typically the responsibility of railroads' operations officers, not the chief information officer's staff. Control systems, i.e., signal systems located in the field (not central office based), are used to monitor train location. Signaling systems typically use both private and public networks, wired and wireless. These communications networks allow the dispatch system to set train routes and provide train location in return. Wayside sensors are used to monitor such things as wheel bearing condition and whether rock slides have impeded the track.

- Also within the transportation sector, the freight transportation industry, which includes trucking, air, rail, and waterborne transportation, uses general purpose business applications to manage internal processes and to link them with internal and external entities, mobile communications and tracking to maintain control over assets, and the Internet for electronic commerce and to link various systems.

- The telecommunications sector uses all forms of information technology, including some specialized systems, for business operations (pay/personnel), infrastructure (providing service to customers), and operational support (monitoring of telecommunications traffic). In addition, entities within this sector provide information technology and IT services to its customers.

Some Infrastructure Entities Utilize Specialized Systems and Technologies

Entities within certain critical infrastructures, such as banking and finance, transportation, chemical, telecommunications, and energy, use technologies that provide them with unique capabilities to perform critical functions. For example, there are centrally and federally controlled systems that allow entities to complete financial transactions, expedite

[15]Dispatching systems provide time slots for trains to enter the rail network. These systems are critical to the operation of the rail network. The dispatching process can no longer be performed manually because the level of operation needed to maintain the flow of the trains, and thus of the goods, is too high to perform without the computers. The first priority of dispatching operators is to maintain safety.

transportation of goods, monitor the location of their assets and goods, and provide for safe travel.

Other information technologies provide entities with the means to monitor or control processes and to monitor the status of assets remotely and without human intervention. Referred to collectively as control systems, they are used by many infrastructures and industries (including electric power generation, transmission, and distribution; oil and gas refining and pipelines; water treatment and distribution; chemical production and processing; railroads and mass transit; and manufacturing) to monitor and control sensitive processes and physical functions. Control system functions vary from simple to complex; they can be used simply to monitor processes—for example, the environmental conditions in a small office building—or to manage most activities in a municipal water system or even a nuclear power plant.

Sectors Have Similar Cybersecurity Requirements but the Specifics Vary

Because infrastructure sectors make use of similar computer and networking technologies, they have similar needs for cybersecurity. However, the level of importance placed on various aspects of cybersecurity varies. For instance, cybersecurity requirements are often described in terms of the confidentiality, integrity, or availability of data and systems. Confidentiality ensures the preservation of authorized restrictions on the access and disclosure of information, including means for protecting personal privacy and proprietary information. Integrity is defined as guarding against improper modification or destruction of information, and includes information nonrepudiation and authenticity. Availability means ensuring timely and reliable access to and use of information.

We found that sector entities generally share these basic cybersecurity objectives for their systems and networks, but they vary in the relative importance they place in these objectives based on the operational area or function involved. According to sector representatives, the importance placed on these objectives varies depending on the sector's risk assessment, priorities, current regulations, market forces, culture, and history. For example, water industry officials believe that integrity is the most important of the three requirements, while officials from the defense industrial base believe that availability is the most important. In contrast, sector representatives from the chemical industry stated that the importance of confidentiality, integrity, and availability is relative to the task being performed. Chemical sector officials stated that if manufacturing is the task, then integrity is paramount, but if personnel is the task, then confidentiality is the most important. According to electric

power infrastructure representatives, the priority depends on the segment of the business that is referred to—generation, transmission, or distribution. These officials defined the priority order in the generation of power as (1) integrity, (2) availability, then (3) confidentiality. However, in the power-marketing segment of the business, confidentiality is a high priority because of the requirement to keep bids sealed prior to sales.

These factors, in combination with financial factors like costs and benefits, can affect an infrastructure entity's use of IT as well as its need for and deployment of cybersecurity technologies.

Chapter 3: Cybersecurity Technologies and Standards

Critical infrastructure owners use current cybersecurity technologies, such as firewalls and antivirus software, to help protect the information that is processed, stored, and transmitted in the network systems that are prevalent in the infrastructures.[1] To help infrastructure owners purchase cybersecurity technologies, standards are available that describe the operating characteristics and qualities of cybersecurity technology products. Standards that describe protocols and operating guidelines that describe how to use technology products are also available.

Cybersecurity Technologies

The following categories of cybersecurity technology products represent common control elements that help to secure IT systems and networks:

- **Access controls** restrict the ability of unknown or unauthorized users to view or use information, hosts, or networks. Access control technologies can help protect sensitive data and systems. Access controls include boundary protection, authentication, and authorization technologies.

- **System integrity controls** are used to ensure that a system and its data are not illicitly modified or corrupted by malicious code. Antivirus software and integrity checkers are two types of technologies that help to ensure system integrity.

- **Cryptography controls** include encryption of data during transmission and when it is stored on a system. Encryption is the process of transforming ordinary data into a code form so that the information is accessible only to those who are authorized to have access. Two applications of cryptography are virtual private networks and digital signatures and certificates.

- **Audit and monitoring controls** help administrators to perform investigations during and after an attack. We describe four types of audit and monitoring technologies: intrusion detection systems, intrusion prevention systems, security event correlation tools, and computer forensics.

[1]GAO has previously reported on cybersecurity technologies available to help secure federal computer systems. See U.S. General Accounting Office, *Information Security: Technologies to Secure Federal Systems*, GAO-04-467 (Washington, D.C.: March 9, 2004).

- **Configuration management and assurance controls** help administrators to view and change the security settings on their hosts and networks, verify the correctness of security settings, and maintain operations in a secure fashion under duress conditions. We discuss five types of configuration management and assurance technologies: policy enforcement, network management, continuity of operations, scanners, and patch management.

Table 10 lists some of the currently available cybersecurity technologies, organized according to these categories of security controls. Appendix III provides further details on these technologies.

Table 10: Common Types of Current Cybersecurity Technologies

Category	Technology	What it does	Limitations
Access control			
Boundary protection	Firewalls	Control access to and from a network or computer.	Some types of firewalls are vulnerable to spoofing. More complex firewalls require more time to pass message traffic through.
	Content management	Monitors Web and messaging applications for inappropriate content, including spam, banned file types, and proprietary information.	Need to be able to accurately characterize inappropriate content for the filters to maximize matches and minimize false matches. For Web pages, filters may be difficult to keep up-to-date because of the growth of content on the Internet.
Authentication	Biometrics	Uses human characteristics, such as fingerprints, irises, and voices, to establish the identity of the user.	Effectiveness is based on the quality of the devices used. Human characteristics change over time and individuals may need to periodically update their information.
	Smart tokens	Establish identity of users using an integrated circuit chip in a portable device such as a smart card or time synchronized token.	Tokens can be lost or stolen and hence cannot reliably be bound to a specific identity when used in isolation from other methods of authentication.
Authorization	User rights and privileges	Allow or prevent access to data, systems, and actions of users based on the established policies of an organization.	Can be cumbersome to maintain in large organizations. Need to establish an effective balance between reducing unauthorized actions and granting access to resources to those that have a need for them.
System integrity	Antivirus software	Provides protection against malicious code, such as viruses, worms, and Trojan horses.	Because new types of malicious code are discovered on a regular basis, virus signature updates are required on a regular basis. If not updated, antivirus software will not be able to detect new viruses.

Category	Technology	What it does	Limitations
	Integrity checkers	Monitor alterations to files on a system that are considered critical to the organization.	Does not prevent changes to the files, but can provide a record that changes did occur. Effectiveness depends on the accuracy of the baseline. Cannot always distinguish between authorized and unauthorized changes to the baseline.
Cryptography	Digital signatures and certificates	Uses public key cryptography to provide (1) assurance that both the sender and the recipient of a message or transaction will be uniquely identified, (2) assurance that the data have not been accidentally or deliberately altered, and (3) verifiable proof of the integrity and origin of the data.	Management processes such as ensuring the security of private keys and being able to establish trust in certificate authorities are instrumental to the success of this technology.
	Virtual private networks	Allow organizations or individuals in two or more physical locations to establish network connections over a shared or public network, such as the Internet, with functionality similar to that of a private network.	Does not ensure the security of the hosts on either end of the virtual private network. Implementation often requires specialized software or customization of applications.
Audit and monitoring	Intrusion detection systems	Detect inappropriate, incorrect, or anomalous activity on a network or computer system.	Effectiveness is limited by capture of accurate baselines or normal network or system activity. Technology is prone to false positives and false negatives and is not as effective in protecting against unknown attacks. Cannot prevent attacks from damaging the network or host.
	Intrusion prevention systems	Build on intrusion detection systems to detect attacks on a network and take action to prevent them from being successful.	Effectiveness is limited by accuracy of the intrusion detection component. Technology results in reduced throughput through a network.
	Security event correlation tools	Monitor and document actions on network devices and analyze the actions to determine if an attack is ongoing or has occurred. Enable an organization to determine if ongoing system activities are operating according to its security policy.	These tools are limited by their ability to interface with numerous security products. Because of the reliance on logs, new attacks that are not reported on logs may go unseen. Proper access controls to log files are required to maintain their integrity.
	Computer forensics tools	Identity, preserve, extract, and document computer-based evidence.	Technology has no standards from which to judge the validity of results produced by these tools and their admissibility as evidence for law enforcement purposes.
Configuration management and assurance	Policy enforcement applications	Enable system administrators to engage in centralized monitoring and enforcement of an organization's security policies.	Effectiveness is based on security policies. Some applications do not work on all operating systems.
	Network management	Allow for the control and monitoring of networks, including management of faults, configurations, performance, and security.	Must often work with different vendor-specific elements to communicate with its network components.

Category	Technology	What it does	Limitations
	Continuity of operations tools	Provide a complete backup infrastructure to maintain the availability of systems or networks in the event of an emergency or during planned maintenance.	Technologies may be complex to manage.
	Scanners	Analyze computers or networks for security vulnerabilities.	This technology can identify vulnerabilities but does not have the capability to fix them. Cannot identify unknown vulnerabilities.
	Patch management	Acquires, tests, and applies multiple patches to one or more computer systems.	Organization still needs to determine whether patches will negatively affect the operation of target systems. Automated distribution may create a potential security exposure.

Source: GAO analysis.

Access Controls

Boundary protection technologies protect a network or a node by controlling the network traffic at a network boundary—typically the point where an internal network or a node connects to an external network such as the Internet. Typical boundary protection technologies include firewalls and content management tools.

- Firewalls control the network packets that pass between two networks or a network and a node, and can keep unwanted external data out and sensitive internal data in. A firewall acts as a protective barrier because it is the single point through which both incoming and outgoing communications pass. There are many types of commercially available firewalls, including packet filters, stateful inspection firewalls, application proxy gateways, and dedicated proxy servers. Properly configured firewalls provide a level of protection for critical infrastructure systems that connect to the Internet and that are susceptible to cyber attacks from hackers anywhere in the world.

- Content management or filtering technologies can monitor Web, e-mail, and other messaging applications for inappropriate content, such as spam, proprietary information, and banned files types. The technologies can also check for noncompliance with an organization's security policies. These technologies can help keep illegal material out of an organization's systems, reduce network traffic from spam,[2] and stop some forms of cyber attacks. In addition, these tools can track

[2]Spam is electronic junk mail that is unsolicited and usually is advertising for some product.

which users are browsing the Web, when they are doing so, which sites they are viewing, and the duration of time spent at those sites.

Authentication technologies help to establish the validity of a user's claimed identity, typically during access to a system or application (for example, login). Users can be authenticated using mechanisms such as requiring them to provide something they have (for example, a smart card); something they alone know (for example, a password or a personal identification number); or something they are (for example, a biometric). Cryptography is also often used to provide integrity to the authentication process.

- Biometrics cover a wide range of technologies that are used to verify identity by measuring and analyzing human characteristics. Identifying an individual's physiological characteristic is based on measuring a part of the body—such as fingertips and eye irises. Biometrics are theoretically very effective personal identifiers because the characteristics they measure are thought to be distinct to each person.

- Smart tokens are easily portable devices that contain an embedded integrated circuit chip capable of storing and processing data. Smart cards, a type of smart token, contain an embedded microprocessor and can exchange data with other systems. Other types of smart tokens include time-synchronized tokens that generate unique values at regular time intervals and challenge-response tokens that can produce a onetime password based on prompts from a central server.

Once a user is authenticated, **authorization technologies** are used to allow or prevent actions by that user based on predefined rules. Authorization technologies support the principles of legitimate use, least privilege, and separation of duties. These technologies help to define and maintain what actions an authenticated user can perform once granted access to a system. Operating systems have some built-in authorization features such as user rights and privileges, groups of users, and permissions for files and folders. Network devices, such as routers, may have access lists that can be used to authorize those who can access and perform certain actions on the device. Access rights and privileges can be used to implement security policies that determine what a user can do after being allowed into the system.

System Integrity

Antivirus software can help to detect known viruses and worms and stop them before they cause damage to a system's software or data.

Antivirus software provides protection against viruses and malicious code such as worms and Trojan horses. Effective antivirus software should reliably detect and remove viruses and malicious code, in addition to preventing the unwanted effects and repairing the damage that could result. There are several different types of antivirus software, including signature scanning, where the software contains a database of virus signatures and scans files in a computer system for certain "signature strings" that are associated with known viruses. Other technologies scan for lines of computer code that are associated with virus-like behaviors, or check untrusted code for suspicious behavior before it is permitted to execute.

Integrity checking tools can detect whether any critical system files have been changed, thus enabling the system administrator to look for unauthorized alteration of the system. Integrity checkers examine stored files or network packets to determine if they have been altered or changed. These checkers are based on checksums—a simple mathematical operation that turns an entire file or a message into a number. More complex hash functions that result in a fixed string of encrypted data are also used. The integrity checking process begins with the creation of a baseline, where checksums or hashes for clean data are computed and saved. Each time the integrity checker is run, it again makes a checksum or hash computation and compares the result with the stored value.

Cryptography

Encryption technologies can be used on data to (1) hide their information content, (2) prevent their undetected modification, and (3) prevent their unauthorized use. When properly implemented, encryption technologies can provide assurance regarding the confidentiality, integrity, or origin of information that has been exchanged. It can also provide a method by which the authenticity of a document can be confirmed.

Several levels of cryptographic technology are currently in use. Cryptographic modules implement algorithms that form the building blocks of cryptographic applications. Using these modules, technologies are available that can be used to encrypt message transmissions so that eavesdroppers cannot determine the contents of the message. Digital signature technologies use cryptography to authenticate the sender of a message. Hash technologies use cryptography to provide assurance to a message recipient that the contents of the message have not been altered.

Several cryptographic technologies are used to ensure the confidentiality and integrity of data as it is being transmitted over the network. These

technologies include digital certificates, digital signatures, secure sockets layer (SSL), and virtual private networks (VPN). Many of these technologies are built into applications that are commonly available on many computer systems. For example, most Web browsers support SSL for secure communications between a computer and the Web server.

Digital signatures use public key cryptography to provide authentication, data integrity, and nonrepudiation for a message or transaction. Just as a physical signature helps to provide assurance that a letter has been written by a specific person, a digital signature helps provide assurance that a message was sent by a particular individual or machine. A digital certificate is an electronic credential that can help verify the association between a public key and a specific entity.

Virtual private networks allow organizations or individuals in two or more physical locations to establish network connections over a shared or public network, such as the Internet, with functionality similar to that of a private network. VPNs establish security procedures and protocols that encrypt communications between the two end points. VPNs encrypt not only the data but also the originating and receiving network addresses.

Audit and Monitoring

Intrusion detection systems (IDS) and **intrusion prevention systems (IPS)** monitor and analyze events occurring on a system or network and either alert appropriate personnel or prevent the attack in progress from continuing. Both technologies can use a pattern matching algorithm or an anomaly-based algorithm that identifies deviations from normal network or system behavior in order to detect attacks. While an IDS can only provide alerts to an administrator that an attack is occurring, an IPS can take steps to defend against the attack or mitigate its effects.

Security event correlation tools produce audit logs, or lists of actions, that have occurred from operating systems, firewalls, applications, and other devices. Depending on the configuration of the logging functions, critical activities, such as access to administrator functions, are logged and can be monitored for anomalous activity. During an investigation, the logs can be examined to determine the method of entry that was used by an attacker and to ascertain the level of damage that was caused by the attack. Because of the volume of data involved on some systems and networks, correlation tools are available to analyze the logs and identify key information using particular search terms or correlation analysis. These tools can provide a dynamic picture of ongoing system activities

that can be used to confirm that the system is operating in accordance with the organization's security policies.

Computer forensics tools identify, preserve, extract, and document computer-based evidence. They can be used to recover files that have been deleted, encrypted, or damaged. Computer forensics tools are used during the investigation of a computer crime to determine the perpetrator and the methods that were used to conduct the attack. There are two main categories of computer forensics tools: (1) evidence preservation and collection tools, which prevent the accidental or deliberate modification of computer-related evidence, and (2) recovery and analysis tools.

Configuration Management and Assurance

Policy enforcement applications help administrators to define and perform centralized monitoring and enforcement of an organization's security policies. These tools examine desktop and server configurations that define authorized access to specified devices, and they compare these settings against a baseline policy. These applications provide a centralized way for administrators to use other security technologies, such as access control and security event and correlation technologies.

Network management provides system administrators with the ability to control and monitor a computer network from a central location. Network management systems obtain status data from network components, enable network managers to make configuration changes, and alert them of problems. Network management includes management of faults, configurations, performance, security, and accounting.

To provide **continuity of operations**, secure backup tools are available that can restore system data and functionality in the event of a disruption. Typically these products have been used to address naturally occurring problems, such as power outages. But these tools are now being applied to help recover from system problems resulting from malicious cyber attacks. Technologies are also available to help systems and networks continue to operate in spite of an ongoing cyber attack. To keep systems and networks up and running, many procedural and operational techniques, such as redundant systems and high-availability systems, are available.

Scanners are common testing and audit tools, used to identify vulnerabilities in networks and systems as a part of proactive security testing. A wide variety of scanners is available that can be used to probe modems, internet ports, databases, wireless access points, Web pages, and

applications. These tools often incorporate the capability to monitor the security posture of the networks and systems by testing and auditing the security configurations of hosts and networks.

Patch management tools automate the otherwise manual process of acquiring, testing, and applying patches to a computer system. These tools can be used to identify missing patches on systems, deploy patches, and generate reports to track the status of a patch across various computers.

Cybersecurity Standards

Cybersecurity standards can help to provide the basis for the purchase and sale of security products by defining a set of rules, conditions, or requirements that must be met by the products. There are three broad categories of standards that govern cybersecurity technology: (1) protocol security standards, such as IPSEC and Secure BGP; (2) product security criteria, such as Common Criteria protection profiles; and (3) operational guidelines, such as those issued by NIST. Protocol security standards are interface standards that define points of connection between two devices. Product standards establish qualities or requirements for a product to ensure that it will serve its purpose effectively. Operational guidelines define a process to be followed in order for a security process or system to perform effectively.

Designers and builders of products can use protocol and product standards to create and test products to ensure that they meet the criteria set forth by the standards. Buyers can select standards-compliant technology with assurance that the technology meets the standards. There is considerable interest in cybersecurity standards on the part of governments, industry associations, and the Internet Engineering Task Force. However, precise definitions are needed to test whether standards have been met or not. Such precise definitions are often difficult to articulate for cybersecurity.

Nevertheless, the development and use of a standard can attract a scrutiny that helps to reduce design flaws and promote security. Additionally, the existence of standards promotes the availability of detailed technical information about a technology, which may serve as a basis for determining where vulnerabilities remain. At the same time, however, an attack against a specific standard-conforming technology can succeed against all systems that use the standard. On the other hand, a single countermeasure could protect all standards-compliant systems. Thus, standards can help as well as hurt cybersecurity. Overall, standards would be useful in promoting cybersecurity because they would make it possible

for organizations, including the federal government, to purchase cybersecurity technologies that meet minimum standards.

Technology standards are developed and adopted in a number of ways. First, there are national and international standards bodies such as the American National Standards Institute (ANSI) and ISO that typically administer and coordinate voluntary standardization efforts. ANSI is a private, nonprofit organization that promotes and facilitates voluntary consensus standards and conformity assessment systems and safeguards their integrity. ISO is a network of national standards institutes from 148 countries that works in partnership with international organizations, governments, industry, and business and consumer representatives to develop technical standards.

Professional organizations such as the Institute of Electrical and Electronics Engineers (IEEE) and the American Society for Testing and Materials (ASTM) develop technical standards in their areas of expertise. For example, there are IEEE standards for networking technologies such as Ethernet over many different media, including wireless.

A different standards process drives the Internet standards that are related to protocols, procedures, and conventions that are used in or by the Internet. Internet standards begin life as a specification written in the form of a Request for Comments (RFC) document. The RFC undergoes a period of development, several iterations of review by the Internet community, and revision based on experience. Then it is adopted as a standard by the Internet Engineering Steering Group and is published. The detailed Internet standards process itself is documented as an RFC.[3]

Government agencies are also involved in developing and promoting standards. For example, in the federal government, NIST has the mission to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST is leading the development of key information system security standards and guidelines as part of its FISMA Implementation Project. This includes the development of Federal Information Processing Standards (FIPS) that apply to information systems built or acquired by the civilian agencies in the federal government. NIST also publishes many special publications on

[3]Bradner, Scott, *The Internet Standards Process—Revision 3*, RFC 2026 (Oct. 1996).

computer security that provide guidance to federal agencies on many aspects of computer security.

Table 11 lists examples of current cybersecurity standards, organized by high-level control categories.

Table 11: Examples of Cybersecurity Standards

Control category	Standards
Access controls	Boundary Protection • Network Address Translation (RFC 3022) • SOCKS Protocol Version 5 (RFC 1928)
	Authentication • IP Security Protocol (IPSEC) • DNS Security Extensions (DNSSEC) (RFC 2535) • SNMPv3 Security (RFC 3414) • IEEE P1363 PKI standards • A One-Time Password System (RFC 2289) • ISO/IEC 7816: Smart Card Security • ISO 9798-1: Security Techniques—Entity Authentication Mechanism
	Authorization • CCITT X.500 directory standard
System integrity	Integrity • Federal Information Processing Standard (FIPS) 198: The Keyed-Hash Message Authentication Code (HMAC) March 2002 • FIPS 180-2: Secure Hash Standard (SHS), (SHA-1, SHA-256, SHA-384, and SHA-512) • ISO 10118-1: Security Techniques—Hash Functions Non-repudiation—digital signature • FIPS 186-2: Digital Signature Standard (DSS) • ANSI X9.31-1998: Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry • ANSI X9.62-1998: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm • ISO 9796: Security Techniques—Digital Signature Scheme Giving Message Recovery • ISO 13888-1: Security Techniques—Non-repudiation • ASTM E2084-00: Standard Specification for Authentication of Healthcare Information Using Digital Signatures
Cryptography	Encryptionalgorithms • RSA Public Key Cryptography Standards (PKCS) • FIPS 197: Advanced Encryption Standard (AES) • FIPS 46-3: Data Encryption Standard (DES) • ANSI X9.52-1998: Triple Data Encryption Algorithm Modes of Operation • FIPS 185: Escrowed Encryption Standard (EES)-Skipjack

Control category	Standards
	Encrypted transmission • Secure Sockets Layer (SSL) v3.0 • Transport Layer Security (TLS) v.1 (RFC 2246) • IP Security Protocol (IPSEC) and IKE (Internet Key Exchange) (RFC 2409) • Secure Shell (SSH) • Layer Two Tunneling Protocol (L2TP) for VPN (RFC 2661) • IEEE 802.11 and 802.11i (in process) • Wi-Fi Protected Access (WPA) Encrypted storage • OpenPGP Message Format (RFC 2440) • MIME Security with OpenPGP (RFC 3156)
Audit and monitoring	Intrusion detection • The Intrusion Detection Exchange Protocol (IDXP), Internet Draft
	System event correlation tools • ASTM E2147-01: Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
Configuration management and assurance	Network management • Simple Network Management Protocol (SNMP) (RFC 3416)

Source: GAO analysis.

A number of other security standards and guides cover more than one of the control categories shown in table 11. One good example is ISO 17799, which is a standard for information security management.[4] Some sectors, such as the health care sector, have their own guides, such as ASTM E1762, *Standard Guide for Electronic Authentication of Health Care Information*.[5]

[4]International Organization for Standardization, *Information Technology – Code of Practice for Information Security Management*, ISO 17799 (2000). ISO 17799 is a widely recognized information security standard and is described as a "comprehensive set of controls comprising best practices in information security".

[5]ASTM International, *Standard Guide for Electronic Authentication of Health Care Information*, ASTM E1762 (2003).

Another well-known security standard is the Information Technology Security Evaluation Criteria, also known as the Common Criteria.[6] European and North American governments are moving toward Common Criteria as a unified set of security criteria. Version 2 of the Common Criteria attempts to reconcile a number of existing criteria, including the United States Trusted Computer System Evaluation Criteria, the so-called Orange Book criteria. Common Criteria has two underlying dimensions: (1) the protection profiles that capture the security functionality, and (2) the evaluation assurance level that specifies how much to trust the claims of the security profile.

Standards such as the Common Criteria are written in general terms because the criteria must cover a variety of products and technologies. When such criteria are applied to a specific product, the criteria must be interpreted, and it is the interpretation that sets the level of security that the product must meet.

NIST and NSA are undertaking a collaborative effort, the National Information Assurance Partnership (NIAP), to produce comprehensive security requirements and security specifications for key technologies that will be used to build more secure systems for federal agencies. These security requirements and security specifications will be developed with significant industry involvement and will employ the Common Criteria. Protection profiles in key technology areas such as operating systems, firewalls, smart cards, biometrics devices, database systems, public key infrastructure (PKI) components, network devices, virtual private networks, intrusion detection systems, and Web browsers will be the primary focus of this project.

The NIAP Common Criteria Evaluation and Validation Scheme Web site also provides information about Common Criteria-validated products, validated protection profiles, products that are in evaluation, and protection profiles that are in development.[7] For example, some of the

[6]Common Criteria consists of three ISO standards: ISO 15408-1 *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 1: Introduction and General Model* (1999); ISO 15408-2 *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 2: Security Functional Requirements* (1999); and ISO 15408-3 *Information Technology— Security Techniques—Evaluation Criteria for IT Security—Part 3: Security Assurance Requirements* (1999).

[7]Validated product lists are available online at the Common Criteria Evaluation and Validation Scheme Web site at http://niap.nist.gov/cc-scheme/ValidatedProducts.html.

validated product types include switches, routers, wireless local area networks, firewalls, virtual private networks, operating systems, antivirus software, biometrics, and intrusion detection systems. Validated U.S. government protection profiles exist for a number of security technologies such as firewalls, operating systems, smart card tokens, and intrusion detection systems.

In addition to supporting Common Criteria evaluations of products, NIST operates the Cryptographic Module Validation Program (CMVP), which uses independent, accredited, private sector laboratories, to perform security testing of cryptographic modules for conformance to FIPS 140-2, *Security Requirements for Cryptographic Modules*, and related federal cryptographic algorithm standards. A government body validates the results of the CMVP testing, and evaluation processes to ensure that the security standards are being applied correctly and consistently.

Unfortunately it takes time and money to evaluate products against the Common Criteria. There is a shortage of evaluated components, and there is little or no rigorous methodology for assessing the security of systems composed of components that have been evaluated using the Common Criteria. Further, with an ever increasing number of threats emerging, Common Criteria protection profiles would need to be regularly updated to ensure that products certified with the criteria remain secure.

Chapter 4: Cybersecurity Implementation Issues

Critical infrastructure owners are ultimately responsible for addressing their cybersecurity needs. However, as we have described, there are several other stakeholders involved with efforts to enhance cybersecurity. For some infrastructure sectors, sector coordinators—individuals or organizations—perform a collective role in helping the entities within their sector to improve cybersecurity. In addition, federal, state, and local governments have a stake in ensuring that the interests of national security and the public good are addressed, and they have a variety of policy tools that can be used to influence how the nation's critical infrastructures are protected, including regulations, grants, and partnerships. In some cases, the federal government plays an important role in the operations of a critical infrastructure sector. For example, the Federal Aviation Administration's (FAA) air traffic control system is essential to the operations of the aviation transportation sector. IT manufacturers, including cybersecurity technology companies, develop and market the tools used by critical infrastructure owners to conduct their business and protect their information technology infrastructure from security risks. All of these parties face various challenges in addressing the nation's cybersecurity needs. Such challenges range from identifying cybersecurity problems within an organization to creating business cases so that specific cybersecurity technologies can be deployed in or developed for it. Many of these challenges are common to all types of critical infrastructures while some challenges are unique to specific sectors. Concomitant with the challenges, there are opportunities for action by the federal government, critical infrastructure sectors, individual entities that own critical infrastructures, and technology manufacturers.

This chapter focuses on two major categories of potential actions for improving cybersecurity for CIP. First, the implementation of available cybersecurity technologies and processes could help address critical infrastructure owners' immediate cybersecurity needs. We present cybersecurity challenges that are faced by critical infrastructure owners and suggest approaches and actions that are available to help meet those challenges, including the use of cybersecurity technology.

Second, we discuss policy options available to the federal government that can make more cybersecurity technologies available and encourage their use by infrastructure owners. Several activities have already been undertaken by the federal government and by critical infrastructure sectors to improve critical infrastructure protection. To determine whether to continue or expand current programs or to develop new cybersecurity programs, it would be useful to examine the effectiveness of these current activities and assess whether further investment is required.

Further, an important common thread in all the opportunities for actions is the certainty of consequences—both intended and unintended—of any policy action. Before proposing or implementing any policy action, the federal government needs to consider these potential consequences, as well as the costs and benefits of the action.

A Risk-Based Framework for Infrastructure Owners to Implement Cybersecurity Technologies

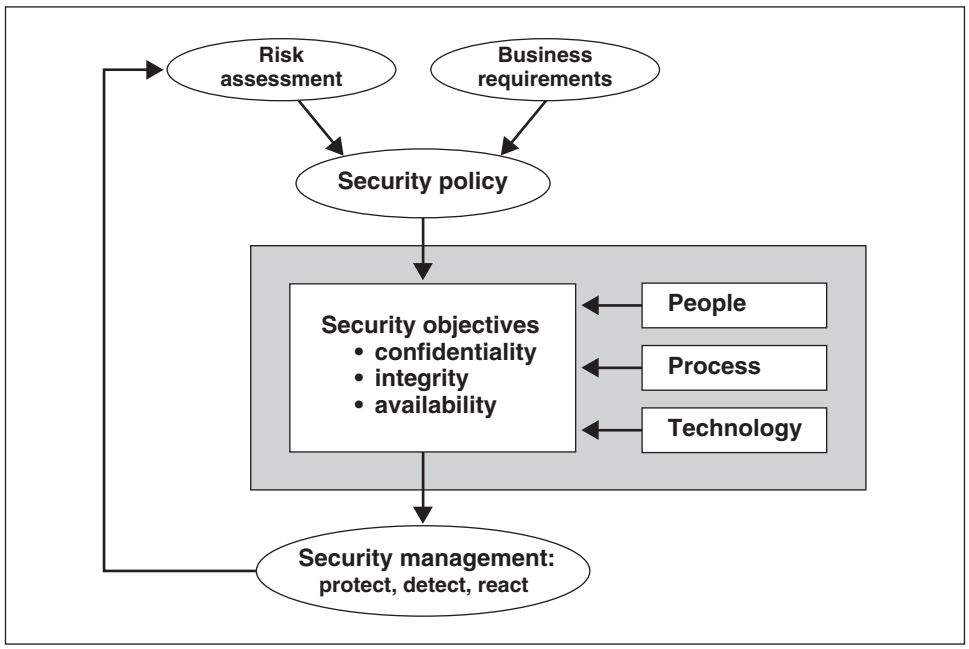
A basic challenge facing critical infrastructure owners is that they have to address many different issues that affect their operations. Security issues, both physical and cyber, are only one element of what affects an entity's operations. Management's primary concern is the day-to-day operation, the investments needed for the future, and stakeholder, stockholder or owner satisfaction with its performance. An overall security framework can help an entity properly evaluate the importance of cybersecurity problems within the context of its operations. Security best practices recommend that a risk assessment methodology be used to make informed security investment decisions. If an entity has not conducted a risk assessment, it cannot know the extent of its cybersecurity problem. Even when it knows the extent of cybersecurity needs, it cannot protect everything. Further, an entity often needs a business case to invest in cybersecurity.

On the basis of the results of a risk assessment, infrastructure owners can implement available cybersecurity technologies to mitigate identified risks. There are several categories of cybersecurity technologies available that could be used to better secure critical infrastructure systems. However, infrastructure owners also need to bear in mind the limitations of these technologies, as well as the interactions of the technologies with the security processes and the people using the technologies.

Using an Overall Framework for Cybersecurity

It is important to think of cybersecurity in an overall framework (see figure 4) that includes the following processes: (1) determining the business requirements for security; (2) performing risk assessments; (3) establishing a security policy; (4) implementing a cybersecurity solution that includes people, process, and technology to mitigate identified security risks; and (5) monitoring and managing security continuously.

Figure 4: An Overall Framework for Security



Source: GAO analysis.

A cybersecurity framework starts with the development of a security policy based on business requirements and a risk analysis. The business requirements identify the needs of the enterprise, including cybersecurity requirements—the computer resources and information that have to be protected, including any requirements imposed by applicable laws, such as HIPAA, FISMA, and requirements to protect the privacy of some types of data. Some risks are external to the entity conducting the risk assessment and involve considerations beyond the risks that are within the entity's control.

On the basis of the risk analysis and the business requirements for cybersecurity, an entity can develop its security policy. Such a security policy typically addresses high-level objectives such as ensuring the confidentiality, integrity, and availability of data and systems. As we previously described, we found that sector entities generally share these basic cybersecurity objectives for their systems and networks, but they vary in the relative importance they place on these objectives based on the operational area or function involved.

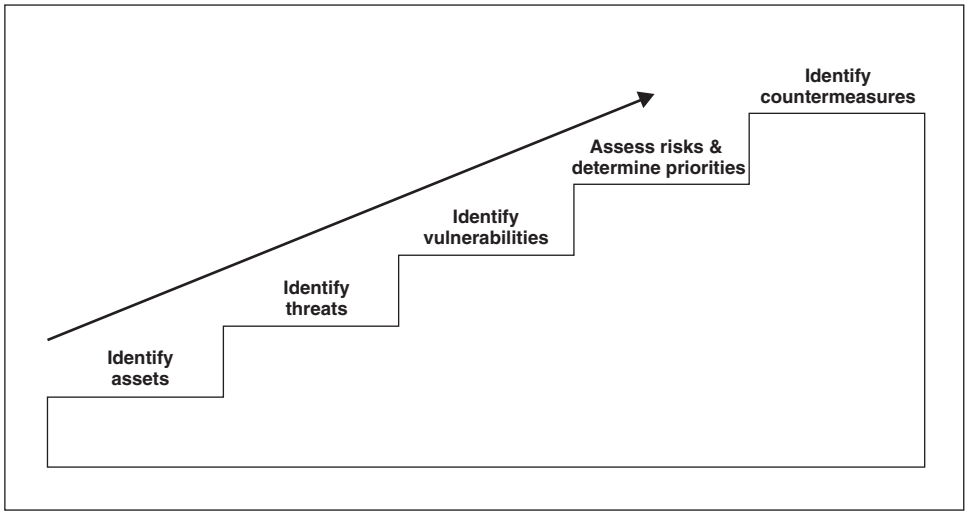
These security objectives are achieved by implementing cybersecurity solutions that make use of people, process, and technology. Because of the variation in cybersecurity objectives among critical infrastructure sectors, while the types of IT and cybersecurity technologies are the same across all sector entities, the details of implementation and the level of their use differ from one sector to another. In addition to implementing security solutions, entities need security management that continuously protects against, detects, and reacts to any security incidents. The combination of risk analysis, security policy, security solutions, and security management provides the overall cybersecurity framework and represents a continuous process. Such an overall security framework can help an entity to establish a common level of understanding of its cybersecurity posture and a common basis for the design and implementation of cybersecurity solutions in it.

Risk Assessments Are Key to Cybersecurity Planning

Risk analysis or risk assessment is a key component within the overall framework for cybersecurity. The approach to good security is fundamentally similar, regardless of the assets being protected. As we have previously reported, applying risk management principles can provide a sound foundation for effective security whether the assets are information, operations, people, or federal facilities.[1] A risk management methodology can provide the basic information that is required to make decisions on how to protect an entity's information systems. As seen in figure 5, these principles can be reduced to five basic steps that help to determine responses to five essential questions:

[1]U.S. General Accounting Office, *National Preparedness: Technologies to Secure Federal Buildings*, GAO-02-687T (Washington, D.C.: Apr. 25, 2002).

Figure 5: Five Steps in the Risk Management Process



Source: GAO analysis.

What Am I Protecting?

The first step in risk management is to identify the assets that must be protected and the impact of their potential loss.

Who Are My Adversaries?

The second step is to identify and characterize the threat to these assets. The intent and capability of an adversary are the principal criteria for establishing the degree of threat to the identified assets.

How Am I Vulnerable?

Step three involves identifying and characterizing vulnerabilities that would allow identified threats to be realized. In other words, what weaknesses would allow a security breach?

What Are My Priorities?

In the fourth step, risk must be assessed and priorities determined for protecting assets. Risk assessment examines the potential for the loss of or damage to an asset. Risk levels are established by assessing the impact of loss or damage, threats to the asset, and vulnerabilities.

What Can I Do?

The final step is to identify countermeasures to reduce or eliminate risks. In doing so, the advantages and benefits of these countermeasures must also be weighed against their disadvantages and costs.

One of the roadblocks to understanding the importance of cybersecurity is the lack of solid information on the scope and scale of cyber vulnerabilities and the consequences of cyber attacks. Risk assessment is a key proactive step that can be used to help an entity decide what to do to protect its cyber assets from potential attacks. Risk assessment provides a framework for analyzing alternatives to mitigate risks and implement countermeasures. Instead of reacting to the latest news of vulnerabilities in software, critical infrastructure owners can use the results of risk assessments to proactively take steps to reduce the risks of cyber attacks. It is important to note that it is not practical or possible to eliminate all risks. There will always be some level of risk that cannot be mitigated without unacceptably large expenditures or the use of overly obtrusive controls.

Risk assessments can be conducted by both sector-wide organizations and critical infrastructure owners. A sector's risk assessment should be based on its knowledge of its exposure to various threats, and it should provide guidance to infrastructure owners on which risks may apply to them. Some infrastructure sectors have completed risk assessments for their sector. For example, the rail segment of the transportation infrastructure sector performed a terrorism risk analysis and related security management plan that provides recommended actions under various alert levels.

Critical infrastructure owners in each sector also conduct risk assessments for their own enterprise and develop mitigation approaches based on available countermeasures. For example, entities within the electric, banking and finance, and chemical sectors have performed risk assessments. These infrastructure owners periodically reassess threats and vulnerabilities after implementing the countermeasures. Thus, risk assessment is a continuing task for any entity that has responsibility for protecting critical infrastructures.

However, while risk assessment is a commonly accepted practice, not all sector entities employ it. Some entities do not even know which of their assets need to be protected, while others have not conducted a vulnerability assessment. Entities in some sectors seem more accustomed than others to using risk assessments for cybersecurity. For example, the banking and finance sector routinely performs risk assessments in the conduct of its business, so its culture seems better suited to taking a risk-based approach to cybersecurity. In addition, regulations require banks to be proactive about cybersecurity monitoring and response.

Risk is the combination of two probabilities: (1) the probability that a threat exists that will locate and exploit a vulnerability and (2) the probability that the threat will succeed in its attempt. A combination of the threat, the vulnerability being exploited by the threat, and the effect of a realized threat can guide entities to mitigate the greatest security risks. Because infrastructure entities have limited resources, a risk management approach can help them focus their efforts on those areas most at risk.

To conduct risk assessments, entities need information about threats and vulnerabilities. Vulnerability information is documented in a variety of publicly available sources. Some well-known online resources that identify and categorize cybersecurity vulnerabilities include the following:

- CERT/CC analyzes vulnerabilities and issues advisories on the most urgent of problems. For less critical problems, CERT/CC publishes incident notes and vulnerability notes.[2]

- Common Vulnerabilities and Exposures (CVE) is a list of standardized names of vulnerabilities.[3] It is common practice to use CVE names to describe vulnerabilities.

- The ICAT Metabase is a searchable index of information on computer vulnerabilities, published by NIST.[4] The ICAT vulnerability index lists over 6,200 vulnerabilities, and it provides links to vulnerability advisories and patch information for each vulnerability.

[2]The CERT/CC vulnerability notes database can be accessed at http://www.kb.cert.org/vuls/.

[3]Common Vulnerabilities and Exposures is available online at http://cve.mitre.org/.

[4]The ICAT Metabase is available online at http://icat.nist.gov/.

- The SANS Institute publishes the SANS/FBI Top 20 List—a list of the 20 most critical Internet security vulnerabilities that is updated periodically.[5]

Sector entities can identify relevant cyber vulnerabilities based on their understanding of the assets in their system environment. The President's *National Strategy for Homeland Security* states that comprehensive vulnerability assessments of all of our nation's critical infrastructures are important from a planning perspective because they can enable authorities to evaluate the potential effects of an attack on a given sector and then invest accordingly to protect it. Without a vulnerability assessment, sector entities will not have a comprehensive approach to determine what parts of their information technology infrastructure require security investments. While some vulnerabilities may be addressed in such an ad hoc manner, it will be difficult to know with any certainty that those vulnerabilities that could cause the greatest harm or are most likely to be exploited have been addressed.

A more proactive testing approach can also be used to identify system vulnerabilities. Sector entities can use automated vulnerability scanning tools that scan a group of hosts or a network for known vulnerable services. Another approach is to conduct a security test and evaluation. Such an approach entails the development and execution of a plan to test the effectiveness of the security controls of IT systems. Penetration testing can also be employed to test for unknown problems. The objective of penetration testing is to test systems and networks from the viewpoint of a threat and identify potential failures in the security control environment.

Although the general threats to cybersecurity are well known, the specific threats to each critical infrastructure sector may not be readily apparent to the entities within the sector. While some sectors have their own threat assessment capability, other sectors rely on the government to provide them with information on threats. It is critical to ensure that appropriate intelligence and other threat information, both cyber and physical, is received from the intelligence and law enforcement communities. Since the 1990s, the national security community and the Congress have identified the need to establish analysis and warning capabilities to protect against strategic computer attacks on the nation's critical computer-dependent infrastructures. Such capabilities should address both cyber

[5]The SANS/FBI Top 20 List is available online at http://www.sans.org/top20/.

and physical threats and involve (1) gathering and analyzing information for the purpose of detecting and reporting otherwise potentially damaging actions or intentions and (2) implementing a process for warning policy makers and allowing them time to determine the magnitude of the related risks.

During a risk assessment, it is important to consider the threat that insiders pose to critical infrastructures. As we have described, because of the access that insiders have to an organization's computer systems, the damage that can be caused by them can be severe. Several steps can be taken to prevent insiders from causing damage to a system. Placing limits on access to sensitive systems and information and separating the duties of employees can minimize the damage that an insider can cause. In addition, organizations can maintain and review reliable logs that track user actions. Technologies can also be used that help to secure the sensitive systems and detect unauthorized access.

Risk assessment also requires an estimate of the consequences of a risk. This entails estimating what happens to an entity if a threat succeeds in exploiting a specific vulnerability in its networked information systems. However, it is difficult to estimate the effect of failures caused by cyber attacks. For example, attacks on Internet infrastructures such as the domain name servers can be varied. Corporations that manage their own internal networks may be totally unaffected by such an attack. Even widespread outages may not affect some users if they have access to cached information. There have been many reports highlighting the monetary impact of cyber attacks, but the basis of those costs are not well understood. The inability to predict the consequences of cyber attacks complicates the process of assessing risks.

Protection, Detection, and Reaction Are Integral Security Concepts

Because it is impossible to protect computer systems from all attacks, countermeasures identified through the risk management process must support three integral concepts of a holistic security program: protection, detection, and reaction (see figure 6). Protection provides countermeasures such as policies, procedures, and technical controls to defend against attacks on the assets being protected. Detection monitors for potential breakdowns in the protective measures that could result in security breaches. Reaction, which often requires human involvement, responds to detected breaches to thwart attacks before damage can be done. Because absolute protection from attacks is impossible to achieve, a security program that does not incorporate detection and reaction is incomplete.

Figure 6: Protection, Detection, and Reaction Are All Essential to Cybersecurity

Source: GAO.

There is a variety of cybersecurity technologies available for addressing protection, detection, and reaction. For example, firewalls can protect a network from some attacks as well as detect when those attacks are attempted. However, some aspects of the protection-detection-reaction triad are difficult to support with current technologies and practices. For example, because of limitations in the current Internet environment, the tracking and tracing of cyber attacks is a very difficult task. The ability to identify the source of an attack could allow for a better response and potentially contain the damage caused by the attack. Law enforcement needs this information in order to investigate, collect evidence, and potentially prosecute the perpetrators of the attack.

One key problem is the untrustworthiness of the source IP address in Internet data packets. The source IP address is supposed to be the IP address of the originator of the network message. However, because the Internet was originally designed to be used by trusted users, no authentication of the source of messages was built into internet protocols. It is possible for malicious users to forge the source address of IP packets to obscure the real source of the attack. Further, IP addresses may identify only a computer involved in the attack. Because of the prevalence of

publicly available computers and of weak access controls and authorization policies on private computers, linking a computer to an attack does not necessarily link the attack to a specific person.

Another key problem is that the Internet crosses administrative and geopolitical boundaries. Different organizations administer different parts of the Internet. There is no central administrative authority of the Internet. While there are common technical standards and protocols that need to be followed by each administrative domain, there are different governing structures in each country. Depending on the configuration of routing tables and network traffic, an IP packet can cross multiple administrative and geopolitical boundaries as it journeys to its destination. The tracing of attacks could require cooperation from several administrative organizations of the Internet to obtain information about the packets in question. If an organization is uncooperative and law enforcement has no legal means to ensure its cooperation, it becomes extremely difficult to trace attacks back to their origin. One of the problems is that there are no universal laws or agreements as to what constitutes a cyber attack.

A Business Case Needs to Be Made for Cybersecurity

Best practices for information technology investment recommend that prior to making any significant project investment, information about the benefits and costs of the investment should be analyzed and assessed in detail. It is further recommended that a business case be developed that identifies the organizational needs for the system and provides a clear statement of the high-level system goals. The high-level goals address the system's expected outcomes, such as preventing unauthorized users from gaining access to a system or detecting and logging security breaches. Certain performance parameters, such as transaction times or maximum loads, are also usually specified.

Some critical infrastructure sector representatives told us that it is difficult for them to address cybersecurity unless it makes business sense to do so—that is, the investment is cost-beneficial. Typically this means that investments must generate revenue, save or avoid costs, or increase productivity. In some cases, IT investments are undertaken for non-quantitative reasons, such as strategic impact or because such investments are necessary to protect critical infrastructure important to national security. While most companies realize that information security breaches are bad for business, in some cases, information security managers find it difficult to justify investments in security based only on the fear of attacks.

However, security managers face challenges in providing this type of justification. According to the Institute for Information Infrastructure Protection (I3P), there are insufficient models and a lack of data to support effective decision making. I3P identified the need for additional research and development in the area of economic analysis in its cybersecurity research and development agenda. It states that sound models to assess the costs and benefits of cybersecurity alternatives need to be developed, and that methods are required to better predict the consequences of risk management choices.

Cost-benefit analyses and return-on-investment calculations are the normal methods used to justify investments. Security technology manufacturers and managed security service providers, as well as some researchers, have developed methodologies to perform this type of analysis for security.

Decision makers also lack baseline data on the costs, benefits, and effects of security controls from an economic and technical perspective. While it is possible to determine the costs of security, it is difficult to quantify the value from such investments because good and consistent security metrics are not available. Without metrics, it is difficult to assess the effectiveness of different security options. NIST has developed guidelines on developing security metrics that could be used to help justify security investments.[6] NIST is also developing guidelines for federal agencies to use to support successful integration of security into the capital investment planning process.

Other Needs Compete with Cybersecurity for Resources

Organizations have limited resources—people and money—and consequently, they typically focus on improving cybersecurity only to the extent that those security needs are necessary to continue their business operations or are demanded by their customers. As we have described, in order to maximize the return from these resources, an entity is best served by taking a risk-based view that considers all the risks that the entity faces. According to its own prioritization of these risks, the entity may determine the threat of cyber attacks to be a significant risk that it must mitigate. At this point, the entity can proceed to implement countermeasures to

[6]National Institute of Standards and Technology, *Security Metrics Guide for Information Technology Systems*, NIST Special Publication 800-55 (Gaithersburg, MD: July, 2003).

mitigate the risk of cyber attacks, based on its analysis of the cost-effectiveness of the countermeasures.

On the other hand, an entity may find that the threat of cyber attacks is not its most significant problem. As we have described, not all threats that an infrastructure faces are of the cyber variety—many threats are physical. By using a risk assessment approach, an entity may determine that the combination of threat, vulnerability, and consequences of physical risks outweigh those of cyber risks. The entity may then primarily implement countermeasures to address those risks and pay less attention to cyber risks.

As we have mentioned, most of the critical infrastructure is owned by the private sector. Similarly, most manufacturers of cybersecurity technology are also in the private sector. These organizations balance the competing needs of their own commercial enterprise, national security, and law enforcement.

- **Commercial enterprise needs**. As we have described, investing in cybersecurity has to make business sense. Typically, this means that companies need to see some type of value to the investment, through either increased sales or reduced costs. However, if a company's customers are not asking for security in its products, it is unlikely that the company will build security into its offerings. Even without an appreciable product or service benefit, a company may still be willing to invest in cybersecurity technologies if doing so will reduce its overall cost structure. However, without a noticeable benefit in either increased sales or a reduction in costs, it becomes very difficult for a company to justify an investment in cybersecurity technology.

- **National security needs**. The designation of critical infrastructure includes those systems and assets that are vital to national security, national economic security, or national public health and safety. However, because most of the critical infrastructure is owned and operated by the private sector, the federal government alone cannot ensure the security of these systems and assets. While it may provide assistance, cultivate partnerships, and establish regulations, the federal government relies on the private sector to carry out its critical infrastructure protection responsibilities.

- **Law enforcement needs**. As we have described, it is impossible to achieve 100 percent protection. Therefore, it is necessary to implement detection and response capabilities into a security program. The needs of law enforcement are part of these capabilities. The ability to

successfully prosecute and convict cyber criminals can also act as a deterrent to others. However, such cases require that companies cooperate with law enforcement and be able to provide evidence of criminal behavior. A working group of law enforcement and industry representatives has issued guidelines for evidence collection for computer crimes.[7]

The needs of these three distinct objectives sometimes conflict with one another. The national security needs could motivate a company to invest in protection technologies and strategies, such as firewalls and access control technologies. The law enforcement needs could cause a company to invest in detection technologies such as intrusion detection systems and audit and logging technologies. However, investment in cybersecurity technologies for national security or law enforcement purposes instead of business reasons can be a tough sell in many companies.

Further, to initiate law enforcement actions against the perpetrator of an attack, a company must report the attack. The reporting of an attack could have a negative business effect, and because of that companies may choose not to report attacks. According to a survey conducted by CSI and the FBI in 2003, only 30 percent of respondents reported computer security incidents to law enforcement.[8] Seventy percent of respondents reported that they did not report intrusions to law enforcement because of concerns about negative publicity. Sixty-one percent were concerned that competitors would use information about computer attacks to their advantage.

We found that entities within the different sectors have different motivations for implementing different levels of cybersecurity. In the absence of any specific guidance from government or the infrastructure sector, some infrastructure owners typically focus on what is best for their own business or mission. To help ensure that national security needs are met, it may be necessary for the federal government to reduce the difference between the commercial needs of an entity and the needs of national security and law enforcement by providing incentives such as funding for cybersecurity improvements. Some of the potential

[7]International Association of Chiefs of Police Advisory Committee for Police Investigative Operations, Pricewaterhouse Coopers LLP, Technical Support Working Group, and the United States Secret Service, *Best Practices for Seizing Electronic Evidence, Version 2.0*.

[8]CSI. *2003 CSI/FBI Computer Crime and Security Survey*.

government investments for the public benefit include hardening the Internet, securing the public health network, and making the power grid resilient. Government resources, however, are limited, and these investments need to be prioritized based on the overall criticality of the infrastructures.

Some Risks Are Beyond the Control of Critical Infrastructure Sectors

A vulnerability assessment may find that there are dependencies on systems or infrastructures beyond the control of an entity. For example, several sectors are dependent on the electrical grid and the telecommunications infrastructure. Some sectors are dependent on computer systems that are operated by other sectors or by the federal government. These interconnections could lead to the introduction of vulnerabilities, and they should be accounted for accordingly.

However, because many of these dependencies are beyond the control of the entity, the options for mitigating these potential vulnerabilities may be limited. To account for such a failure, one possible option for dependent entities is to develop a business continuity plan. As part of a risk management process, a business continuity plan can help an entity to identify its most critical business processes and the actions it can take before and during an outage to mitigate potential risks. Depending on the service provided by the external organization, the criticality of the business process, and the cost of the mitigation strategies, an entity could develop an action plan that would allow it to continue business as usual; operate at some degraded, but minimally acceptable, level; or cease operations until the outage is corrected.

Infrastructures Are Interdependent

Critical infrastructures rely on one another to successfully perform their primary functions. As discussed earlier, understanding these interdependent relationships is critical to protecting our nation's economy, security, and public health. *The National Strategy to Secure Cyberspace* discusses the risks posed by interdependent sectors. It states that unsecured sectors of the economy can be used to attack other sectors and that disruptions in one sector may have cascading effects that can disrupt multiple parts of the nation's critical infrastructure.

For example, the banking and finance infrastructure and the federal government have raised concerns about the financial services sector's interdependency with other critical infrastructures, including telecommunications and energy, and the potential negative impact that attacks in those sectors could have on its ability to operate. According to the financial services sector's national strategy, the industry must take into account the effect of damage from disruptions in other critical sectors,

such as telecommunications, electrical power, and transportation. The attacks of September 11, 2001, demonstrated the dependence of the financial services industry on the stability of other sectors' infrastructures. For example, the industry was negatively affected by disrupted communications for its broker-dealers, clearing banks, and other core institutions.[9] In addition, other sectors are dependent on the banking and finance infrastructure. For example, the chemical industry relies on it for currency management and funding.

The August 2003 electricity blackout demonstrated the effect of the water infrastructure's dependency on the electric sector. Wastewater treatment plants in Cleveland, Detroit, New York, and other locations that lacked backup generation systems discharged millions of gallons of untreated sewage, and power failures at drinking water plants led to boil-water advisories in many communities.

According to industry representatives, the chemical sector is dependent on emergency services, information technology and telecommunications, energy, transportation, and banking and finance. For example, it is highly dependent on rail, trucking, and pipeline services for movement of its products. According to the industry, in 2001, more than 760 million tons of chemical products were shipped by domestic truck, rail, water, and other means. In addition, the industry has a strong relationship with emergency services in communities across the United States in order to enhance their ability to respond to emergencies. Entities within the chemical infrastructure are also dependent on each other as suppliers and customers of each other's products. While the chemical infrastructure is reliant on other infrastructures, industry representatives identified several sectors that are dependent on the chemical infrastructure, including

- agriculture for pesticides, insecticides, and fertilizers;
- emergency services for protective equipment and agents;
- food for packaging;
- information and telecommunications for products that protect memory chips;

[9]Banking and Finance Sector, *Defending America's Cyberspace: Banking and Finance Sector: The National Strategy for Critical Infrastructure Assurance*, Version 1.0 (May 13, 2002).

- public health for devices that neutralize weapons of mass destruction; and
- water for water purifiers.

While these examples indicate that the critical infrastructures are interdependent, the full extent of all the interdependencies is hard to determine.

Infrastructures Rely on Federal and Third-Party Systems

Some officials stated that their infrastructures rely on the availability of centrally controlled or federal systems that are essential to critical operations. For example, according to an infrastructure representative, the banking and finance sector relies upon critical systems related to the clearance and settlement activities for open transactions in the wholesale financial market, which are performed by a combination of government-sponsored services, industry-owned organizations, and private sector firms. According to an interagency paper on strengthening the U.S. financial system, the failure of firms that play a significant role in critical financial markets (defined in the paper as federal funds, foreign exchange, and commercial paper; U.S. government and agency securities; and corporate debt and equity securities) to settle their own or their customers' pending material transactions by the end of the business day could threaten the stability of financial markets.[10]

In addition, according to a Transportation Research Board report, the freight industry has links to government agencies, including manifest filings, operating authorities and permits, and electronic funds transfer.[11] For example, ocean carriers must post information on imported cargo on a DHS Bureau of Customs and Border Protection (formerly the U.S. Customs Service) system—the Automated Manifest System (AMS). According a shipping industry representative, there is now a requirement to submit cargo manifests to this system 24 hours before loading in the foreign port for cargoes destined for the United States. He added that AMS

[10]In April 2003, the Federal Reserve, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission issued a study titled *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* to advise financial institutions on steps necessary to protect the financial system. The practices focus on the appropriate backup capacity necessary for recovery and resumption of clearance and settlement for material open transactions in the wholesale financial market.

[11]National Research Council, *Cybersecurity of Freight Information Systems: A Scoping Study* (Washington, D.C.: 2003).

and a related system are becoming the preeminent centralized government data management systems for security prescreening of imported cargoes. Recently, DHS proposed the mandatory electronic submission of advance import cargo information to AMS for all transportation modes. DHS also has proposed that advance information for all export cargoes from the United States be submitted, for all modes, to the agency's Automated Export System, to enhance cargo security. According to a shipping industry official, disabling one or more of these systems could have results at least as disastrous as those of a physical attack on the maritime infrastructure by stopping the flow of goods. The importance of the Global Positioning System (GPS) to the transportation sector has also been pointed out in multiple reports.[12] DoD maintains GPS, which includes 24 satellites and provides high levels of accuracy in determining Earth positions using triangulation principles and land-based receivers. GPS is used to track the locations of trailers, trucks, railcars, and other mobile assets and their contents.

The aviation-related segments of the transportation infrastructure rely on the availability of the air traffic control system to safely and efficiently move people and goods. The U.S. civil aviation system comprises thousands of airports and aircraft and over 12 million flights each year that carry over 60 million passengers. To carry out its duties, the FAA has approximately 50,000 employees who oversee federal interests in the national airspace system, working at more than 5,000 public use airports. In addition, federal information systems are in use at over 38,000 facilities. These systems are relied on for both passenger and commercial air transportation. Air traffic control systems are responsible for overseeing and tracking most air traffic, including both departing and approaching aircraft. FAA systems provide information to aircraft regarding weather, routes, terrain, and flight plans. There would be detrimental effects on the national economy and possibly on passenger safety if these systems did not function properly.

[12]NRC, *Cybersecurity of Freight Information Systems* and the President's National Security Telecommunications Advisory Committee, *Information Infrastructure Group Report* (June 1999).

Considerations for Implementing Current Cybersecurity Technologies

In the near term, critical infrastructure owners face the challenge, based on risk assessments, of developing and implementing strategies to mitigate identified risks. Risk mitigation strategies are a matter of trade-offs among different options, such as adding security to a large number of products, adding significant security features to a few selected products, or increasing the ability to identify and quarantine attackers.

As we have described, there are several cybersecurity technologies that can be used to improve the security posture of critical infrastructure owners. Organizations can select from and implement available cybersecurity technologies to mitigate the highest cybersecurity risks. Best practices recommend that technologies be selected and implemented in the context of an overall security management process that is designed to address the identified risk mitigation strategy. Individually, these technologies address specific cyber vulnerabilities, and in this sense, each technology is a point solution. The selection of multiple technologies should be in the context of the overall system and not aimed solely at specific components of the system.

When implementing cybersecurity technologies, it is important to consider the effects of the technologies and processes on the entity's business. The entity has to balance security against the level of service that the computers and network must provide in order to operate the critical infrastructure. In other words, a system that is not connected to any network is safe from cyber attacks, but it may not do anything useful for the critical infrastructure. If an authentication process takes too long, users may try to bypass the process or use different ways to conduct their business. For example, control systems have been cited as being difficult to secure because their limited computing resources cannot support security technologies such as encryption without hindering performance.

Further, when selecting and implementing these technologies, it is important to bear in mind that they are not cure-alls. There are limitations to some of these technologies. Technology is only part of the solution. Poorly trained personnel or ineffective security processes can limit the effectiveness of good technology.

Limitations of Cybersecurity Technologies

It is important to take into consideration the limitations of cybersecurity technologies. Security processes must account for these limitations, and the people responsible for using the technology and implementing the security process need to be aware of these issues.

Some technologies are sold as definitive solutions to cybersecurity problems. However, specific technologies can help to solve only a limited number of problems. For instance, firewalls can control the flow of traffic between networks. However, they cannot protect against threats from within the network. Antivirus software can help protect against viruses and worms but cannot protect the confidentiality of data on a system. A suite of technologies is required to adequately protect most computer systems.

Further, infrastructure owners need to determine how effective technologies really are. Because there is a lack of security standards and metrics, it is difficult for buyers to quantitatively determine the effectiveness and performance of cybersecurity technologies. For example, during our review of biometrics, we found instances in which the performance estimates that vendors provided were far more impressive than those obtained through independent testing.[13]

Also, some technologies, such as biometrics and intrusion detection systems, have to account for exception processing. False matches and false nonmatches sometimes occur with these types of technologies, and procedures need to be developed to handle these situations. Exception processing that is not as good as primary processing could be exploited as a security hole. For example, for the use of smart card technologies, administrators would need to consider how to handle users whose cards are not being recognized. Under what conditions will an administrator allow access to such a user?

Further, the constraints that some IT environments face in using cybersecurity technologies need to be considered. For instance, according to industry experts, the use of existing security technologies, as well as strong user authentication and patch management practices, generally cannot be implemented in control systems because control systems operate in real time, typically are not designed with cybersecurity in mind, and usually have limited processing capabilities. Existing security technologies, such as authorization, authentication, encryption, intrusion detection, and filtering of network traffic and communications require more bandwidth, processing power, and memory than control system components typically have. Because controller stations are generally

[13]GAO-02-687T and U.S. General Accounting Office, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

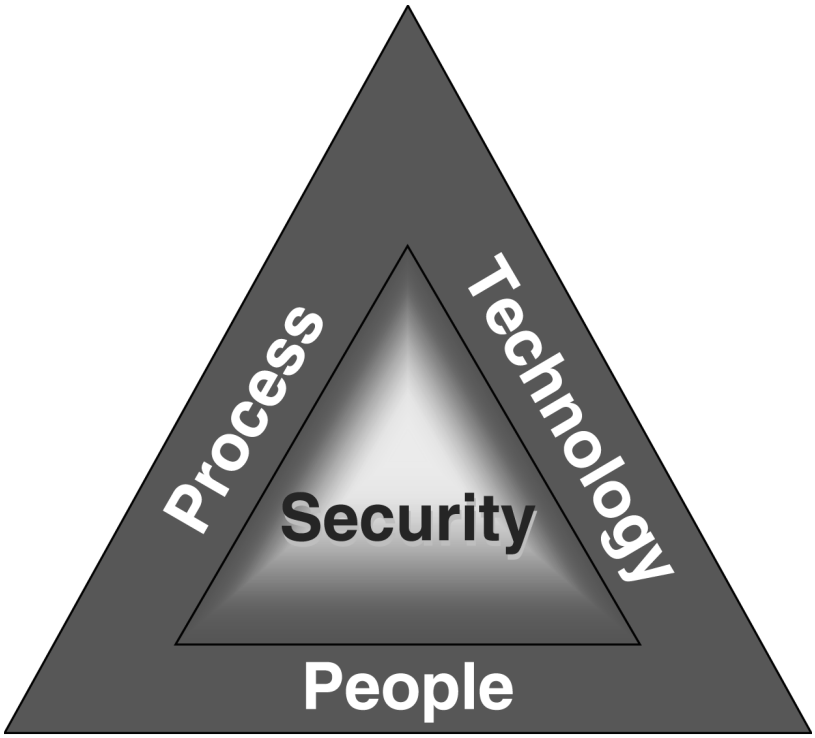
designed to do specific tasks, they use low-cost, resource-constrained microprocessors. In fact, some devices in the electrical industry still use the Intel 8088 processor, introduced in 1978. Consequently, it is difficult to install existing security technologies without seriously degrading the performance of the control system. Further, complex passwords and other strong password practices are not always used to prevent unauthorized access to control systems, in part because their use could hinder a rapid response to safety procedures during an emergency. As a result, according to industry officials, weak passwords that are easy to guess, shared, or infrequently changed are reportedly common in control systems. Sometimes a default password or even no password at all is used.

In addition, although modern control systems are based on standard operating systems, they are typically customized to support control system applications. Consequently, vendor-provided software patches are generally either incompatible or cannot be implemented without compromising service by shutting down "always-on" systems or affecting interdependent operations. Although technologies such as robust firewalls and strong authentication can be employed to better segment control systems from enterprise networks, research and development could help to address the application of security technologies to the control systems themselves. Information security organizations have noted that a gap exists between current security technologies and needed additional research and development to secure control systems.

Poor Implementations Can Reduce the Effectiveness of Cybersecurity Technologies

When implementing technologies, it is important to note that each element of the technology-people-process triad plays a role in the cybersecurity of critical infrastructures (see figure 7). Strong processes can often help to overcome potential vulnerabilities in a security product, while poor implementation can render good technologies ineffective. Often, human weaknesses can diminish the effectiveness of technology. A prime example is the millions of PCs that have unnecessary Internet and networking services running simply because users are unaware that these services are running by default and could contain vulnerabilities.

Figure 7: Technology, People, and Process Are All Necessary for Cybersecurity



Source: GAO.

In our reviews of cybersecurity controls at federal agencies, we have found several instances where the effectiveness of technology was limited through improper configuration of the technology or through human errors. These types of failures can lead to the exploitation of vulnerabilities, resulting in compromised computers and networks.

For example, the most common access control technology is the use of user names and passwords. We have found three common implementation problems in the use of passwords:

- Failure to disable or change default vendor accounts and passwords. In some cases, these accounts could provide a malicious user with administrative privileges.

- Easily guessable passwords, such as children's names or birthdays. Some accounts do not have a password.

- Storage or transmission of user accounts and passwords with weak or no encryption.

Another common issue is the failure of system administrators or security officers to follow procedures:

- Many operating systems and applications provide the capability to log events and transactions, including security-related items such as changes to critical files, network connections, and administrator actions. However, in many cases, we found that logging was not enabled or was not adequately covering enough events. Once logs are created, someone must review them to scan for significant or anomalous activities. However, we have found that logs often are not adequately monitored.

- Patch management, a component of configuration management, is a process used to help mitigate vulnerabilities on computer systems. We have found that reported vulnerabilities on systems frequently remain unpatched. Unpatched systems could allow remote access through a variety of vulnerabilities. For example, we previously reported that almost a month before the Blaster worm attack in August 2003, a patch was made available by Microsoft to address a vulnerability in its Windows Distributed Component Object Model Remote Procedure Call interface.[14] System administrators face challenges in maintaining current technology inventories, identifying relevant vulnerabilities and corresponding patches, and testing and distributing the patches.

Problems also arise when computers and network components are poorly configured. Some examples include the following:

- Key network servers were not adequately configured to restrict access. As a result, anyone, including contractors, with connectivity into the agency network could copy or modify files containing sensitive network information that would allow an intruder to control critical network resources.

- Poorly configured firewalls and internal hosts allowed anyone on the Internet to connect and shadow internal user sessions.

[14]U.S. General Accounting Office, *Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, GAO-03-1138T (Washington, D.C.: Sept. 10, 2003).

- Poorly configured world-writable file permissions allowed Trojan horse programs to be installed using a low-level account to gain administrator privileges.

Poor configuration management has also led to the introduction of vulnerabilities. For example:

- Unbeknownst to the administrators, server configurations had unnecessary services running on them. Because the administrators did not know about these applications, they did not know that patches were required to address vulnerabilities in those applications.

- Dial-in modems did not require passwords to access the internal agency network, thereby circumventing the security controls provided by the firewalls.

- In some instances outdated software versions were exploitable from the Internet. These could be used by an attacker to bypass firewall controls and to launch attacks against other computers in the network.

Configuration management is particularly important for organizations that perform some form of security testing, including the certification and accreditation of systems. Configuration management involves the identification of all software and hardware components of a system at a given point in time and systematically controlling changes to that configuration. Effective security testing loses its value when there is no assurance that the system that is being used in the operational environment is the same system that was successfully tested.

Best Practices and Guidelines Are Available to Select and Implement Current Technologies

When implementing cybersecurity technologies and processes, organizations can avoid making common implementation mistakes by consulting best practices and guidance developed by various other organizations. While federal agencies are required to follow certain security guidelines issued by NIST, private sector organizations may also benefit from these guidelines.

Recently, NIST published a guide on selecting information technology security products.[15] The guide presents the types of products, product characteristics, and environment considerations for each of the following categories of products: identification and authentication, access control, intrusion detection, firewalls, PKI, malicious code protection, vulnerability scanners, forensics, and media sanitizing. NIST has also published a number of other guides on implementing security products.[16] For example, it has guides on electronic mail security and wireless network security, as well as on firewalls and intrusion detection systems.[17]

Other federal agencies, such as the Defense Information Systems Agency (DISA) and NSA have prepared implementation guides to help their administrators configure their systems in a secure manner.[18] Guides exist for the configuration of operating systems such as Windows, UNIX, and OS/390.

Some industry groups have also developed best practices and guidelines to help their member entities implement cybersecurity. For example, the Network Reliability and Interoperability Council (NRIC), a Federal Communications Commission advisory committee, has developed a number of best practices to enhance the reliability of the nation's public communications networks and services.[19] These best practices include homeland security best practices, which in turn include cybersecurity best practices for the telecommunications sector and Internet services. These cybersecurity best practices include a wide variety of specific practices,

[15]National Institute of Standards and Technology, *Guide to Selecting Information Technology Security Products*, NIST Special Publication 800-36 (Gaithersburg, MD: Oct. 2003).

[16]For a list of NIST Special Publications, as these guides are called, see the NIST Web site at http://csrc.nist.gov/publications/nistpubs/.

[17]National Institute of Standards and Technology, *Guidelines on Electronic Mail Security*, NIST Special Publication 800-45 (Gaithersburg, MD: Sept. 2002); *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, NIST Special Publication 800-48 (Gaithersburg, MD: Nov. 2002); *Guidelines on Firewalls and Firewall Policy*, NIST Special Publication 800-41 (Gaithersburg, MD: Jan. 2002); and *Intrusion Detection Systems*, NIST Special Publication 800-31 (Gaithersburg, MD: Nov. 2001).

[18]For DISA's security technical implementation guides, see http://csrc.nist.gov/pcig/cig.html. For NSA's security recommendation guides, see http://www.nsa.gov/snac/index.html.

[19]The NRIC best practices are available online at http://www.nric.org/.

such as disabling unnecessary network-accessible services, using strong encryption algorithms and keys, and defining a security architecture.

In addition, some sectors have issued guidelines to assist entities within the sector in improving their security posture. For example, NERC, the sector coordinator for the electric sector, created *Security Guidelines for the Electricity Sector* as a collection of practices for protecting critical facilities against a range of physical and cyber threats.[20] Its topics include vulnerability and risk assessment, business continuity, physical and cyber security, and protection of sensitive information. The cybersecurity subcategories are risk management, access controls, information technology firewalls, and intrusion detection. In addition, one segment of the chemical industry has a mandatory security code to address security issues within the business of chemistry.[21] The code's purpose is to help protect people, property, products, processes, information, and information systems by enhancing security, including security against a potential terrorist attack, throughout a company's activities that are associated with the design, procurement, manufacturing, marketing, distribution, transportation, customer support, use, recycling, and disposal of products. This code is intended to help companies achieve continuous improvement in security performance using a risk-based approach to identify, assess, and address vulnerabilities; prevent or mitigate incidents; enhance training and response capabilities; and maintain and improve relationships with key stakeholders. It requires each company to implement a risk-based security management that includes the following 13 management practices:

1. **Leadership commitment**—senior leadership commitment to continuous improvement through published policies, provision of sufficient and qualified resources, and established accountability.

2. **Analysis of threats, vulnerabilities, and consequences**—prioritization and periodic analysis of potential security threats, vulnerabilities, and consequences, using accepted methodologies.

[20]North American Electric Reliability Council, *Security Guidelines for the Electricity Sector*, Version 1 (Princeton, NJ: June 14, 2002).

[21]American Chemistry Council, *Responsible Care Security Code of Management Practices* (July 1, 2002).

3. **Implementation of security measures**—development and implementation of security measures commensurate with risks, taking into account inherently safer approaches to process design, engineering and administrative controls, and prevention and mitigation measures.

4. **Information and cybersecurity**—recognition that protecting information and information systems is a critical component of a sound security management system.

5. **Documentation**—documentation of security management programs, processes, and procedures.

6. **Training, drills, and guidance**—enhancing awareness and capability of employees, contractors, service providers, value chain partners, and others, as appropriate.

7. **Communications, dialogue, and information exchange**—sharing information on appropriate security issues with stakeholders such as employees, contractors, communities, customers, suppliers, service providers, and government officials and agencies, balanced with safeguards for sensitive information.

8. **Response to security threats**—evaluation, response, reporting, and communication of security threats as appropriate.

9. **Response to security incidents**—evaluation, response, investigation, reporting, communication, and corrective action for security incidents.

10. **Audits**—assessing security programs and processes and the implementation of corrective actions.

11. **Third-party verification**—third-party verification that, at chemical operating facilities with potential off-site impacts, companies have implemented the physical site security measures to which they have committed.

12. **Management of change**—evaluation and management of security issues associated with changes involving people, property, products, processes, information, or information systems.

13. **Continuous improvement**—continuous performance improvement processes entailing planning, establishment of goals and objectives, monitoring of progress and performance, analysis of trends and development, and implementation of corrective actions.

Further, the oil and natural gas segment of the energy infrastructure sector has security guidelines available that include guidance on cybersecurity.[22] The guidance provides a means to improve the security of the oil and natural gas industry from cyber terrorism and to effectively allocate resources. It also endorses the use of ISO/IEC International Standard 17799 on information security management as a voluntary framework to protect the industry against cyber terrorism.

Considering Security when Developing Systems

To build security into a system, NIST recommends that security requirements for a system be considered as early as possible in the system development life cycle (SDLC).[23] According to NIST, security should be considered as early as the needs determination stage of an IT acquisition or development. A high-level description of the security controls of the proposed system should be included as a part of the preliminary requirements definition for the whole system, which will drive the scoping of the entire effort. If the system acquisition or development is approved, NIST describes several additional steps for considering security, including conducting a risk assessment to derive the security functional and assurance requirements, testing security controls, and certifying and accrediting the system security.

Defense in depth is a common design strategy for protecting computers and networks with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack. Because there are so many potential attackers with such a wide variety of attack methods available, there is no single method for successfully protecting a computer network. Using a strategy of defense in depth can reduce the risk of suffering a successful cyber attack.

[22]American Petroleum Institute, *Security Guidelines for the Petroleum Industry*, Second Edition (Washington, D.C.: Apr. 2003).

[23]National Institute of Standards and Technology. *Security Considerations in the Information System Development Life Cycle*, NIST Special Publication 800-64 (Gaithersburg, MD: Oct. 2003).

In addition, the director, CERT Centers, testified before Congress about the need for "higher quality information technology products with security mechanisms that are better matched to the knowledge, skills, and abilities of today's systems managers, administrators, and users."[24] He added that good software engineering practices can dramatically improve the ability to withstand attacks, and he suggested that the solutions required a combination of

- systems and software that constrain the execution of imported code, especially code that comes from unknown or untrusted sources;
- adoption of known, effective software engineering practices that dramatically reduce the number of flaws in software products; and
- shipment of products with "out of the box" configurations that have security options turned on rather than configurations that require users to turn them on.

Critical Infrastructure Sectors Have Taken Actions to Address Threats to Their Sectors

Federal CIP policy calls for a range of actions intended to improve the nation's ability to detect and respond to serious computer-based and physical attacks and establish a partnership between the federal government and the private sector. It encourages the private sector to voluntarily take efforts to raise awareness, share information, and increase the security posture of their physical and cyber assets. Some infrastructure sectors have taken extensive steps to voluntarily achieve these suggested activities. Considering the current efforts of critical infrastructure sectors can help inform legislative decision making on the need for further government policy making to increase the use of cybersecurity technologies.

Coordination of Efforts and Increasing Participation in Sector Activities

As previously discussed, federal CIP policy states that sector-specific agencies are to continue to support sector-coordinating mechanisms. While some critical infrastructure sectors identified in federal policy have not formally designated a coordinator, including the postal and shipping, public health, food, and agriculture sectors, many other critical infrastructure sectors have established individuals or organizations to coordinate sector-wide activities and initiatives to improve the overall

[24]Testimony of Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University, before the House Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, and Research and Development (June 25, 2003).

cybersecurity of their sectors. For example, banking and finance, telecommunications, information technology, transportation, and water infrastructure sectors and the electricity and oil and natural gas segments of the energy sector have established sector coordinators. In some cases, the sector coordinators are industry associations that represent a large part of the sector. For example, for the electricity segment of the energy infrastructure sector, the North American Electric Reliability Council (NERC) serves as the sector coordinator.[25] According to NERC officials, it represents 100 percent of the entities in the extended regional control area systems, which corresponds to the bulk of U.S. megawatt electricity generation. Also, in the chemical sector, the American Chemistry Council has taken the lead to improve security within the sector.

To ensure the appropriate level of sector participation and build a better consensus on the objectives of the sector-wide efforts, sector coordinators or other key organizations have also taken steps to broaden the involvement of sector entities and relevant trade or industry associations. For example, the financial services sector coordinator organized the Financial Services Sector Coordinating Council for Critical Infrastructure Protection/Homeland Security (FSSCC) to "foster and facilitate the coordination of sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security." It includes major sector associations, professional institutes, national exchanges, and other broad industry organizations that, according to the sector coordinator, provide a way to broaden its membership—potentially reaching more of the approximate 27,000 different financial services entities.[26] In addition, the Chemical Sector Cybersecurity Program was established to enhance cybersecurity throughout the chemical sector value chain in order to help protect people, property, products, processes,

[25]NERC was formed in 1968 and operates as a voluntary industry organization charged with ensuring that the bulk electric system in North America is reliable, adequate, and secure.

[26]Current members of the FSSCC include: the American Bankers Association; the American Council of Life Insurers; America's Community Bankers; ASIS International; the Bank Administration Institute; BITS and the Financial Services Roundtable; Credit Union National Association; the Consumer Bankers Association; the Depository Trust and Clearing Corporation; Fannie Mae; FS-ISAC, the Futures Industry Association; Independent Community Bankers of America; the Investment Company Institute; the Managed Funds Association; NASD, Inc.; the NASDAQ Stock Market, Inc.; the National Association of Federal Credit Unions; the National Automated Clearinghouse Association; the Securities Industry Association; the Securities Industry Automation Corporation/New York Stock Exchange; the Bond Market Association; the Clearing House; the Options Clearing Corporation; and VISA USA, LLC.

information and information systems. The Chemical Sector Cybersecurity Information Sharing Forum consists of senior-level company officials and staff representatives from trade associations and individual companies representing key industry segments within the sector, which serves a critical role in fostering involvement and commitment on the part of chemical companies across the sector.[27] Its objective is to serve as the communications channel for the more than 2,000 chemical companies that constitute the associations' collective membership. In addition, according to an infrastructure sector official, the existing sector coordinators from the various infrastructure sectors have formed a council as the Partnership for Critical Infrastructure Security to coordinate on strategic issues.

Collection and Analysis of Incident, Threat, and Vulnerability Information from Sector Entities

Federal policy recognizes the importance of sharing information about physical and cyber threats, vulnerabilities, and incidents, and continues to encourage the development of ISACs as a mechanism for sharing information. The ISACs recognized by DHS include the following: chemical industry, electric power, energy, financial services, information technology, telecommunications, surface transportation, and water. The ISACs are designed to facilitate information sharing among members by collecting, analyzing, and disseminating information on vulnerabilities, threats, intrusions, and anomalies reported by members, the government, or other sources, in order to avert or mitigate the impact of these factors. Some ISACs consider themselves clearinghouses for information within and among the various sectors. This includes disseminating information technology security information—such as incident reports and warnings, as well as ways to prevent or recover from them. Some ISAC operations are performed completely in-house, while others use contractors to provide warning and analysis functions or simply forward government-issued warnings and alerts. Several provide their members some level of watch services 24 hours a day, 7 days a week. In April 2004, we testified[28] about the management and operational structures used by the 15 ISACs, federal efforts to interact with and support the ISACs, and challenges to

[27]Ten chemical trade associations came together to form this forum, including: American Chemistry Council, Compressed Gas Association, Consumer Specialty Products Association, CropLife America, Dangerous Goods Advisory Council, Institute of Makers of Explosives, National Association of Chemical Distributors, Synthetic Organic Chemical Manufacturers Association, the Chlorine Institute, and the Fertilizer Institute.

[28] U.S. General Accounting Office, *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors*, GAO-04-699T (Washington, D.C.: April 21, 2004).

and successful practices for ISACs' establishment, operation, and partnership with the federal government.

For example, the Financial Services ISAC (FS-ISAC) was formed in October 1999 to, among other objectives, facilitate sharing of information and provide its members with early notification of computer vulnerabilities and attacks. In 2003, the FS-ISAC broadened its mission to serve all financial services sector participants. The goal of the FS-ISAC is to disseminate information on cyber and physical security risks to sector participants on a timely basis. In December 2003, the next generation FS-ISAC was implemented; it includes varying levels of participation, from being a free member to being a premier member ($10,000/year). Available resources to members include early notification of computer vulnerabilities and attacks and access to subject-matter expertise and other relevant information, such as trending analysis for all levels of management and for first responders to cyber incidents.

Another example is the chemical sector ISAC that the American Chemistry Council established in April 2002 to provide a secure facility that allows the sharing of information associated with incidents, threats, vulnerabilities, resolutions, and solutions. It is operated through the American Chemistry Council's 24-hour hazardous material emergency communications center and is linked with DHS's IAIP directorate. According to chemical infrastructure sector officials, the ISAC capability is still in its early development stage regarding cybersecurity.

Also, NERC operates the Electricity Sector ISAC (ES-ISAC), which works with DHS, the Department of Energy, and other entities to help protect the North American electric system from cyber and physical attacks. It is NERC's responsibility to gather, disseminate, and interpret security-related information, operating between industry and the government and among all the sector entities. In addition, the ISAC posts advisories, alerts, warnings, and the current threat alert levels for the Homeland Security Advisory System, the Department of Energy, and the electricity sector.

Further, the railroad industry formed a Surface Transportation ISAC (ST-ISAC). The ST-ISAC operates a 24 x 7 center that collects, analyzes, and distributes critical security and threat information from worldwide resources to protect its members' vital information and IT systems from attack. ST-ISAC reporting includes daily information provided by government intelligence, law enforcement, and regulatory agencies. ST-ISAC services are specifically tailored to meet the security demands of each one of its members. Currently, the ST-ISAC supports almost 200

member entities. ST-ISAC membership consists of more than 90 percent of the North American freight railroad industry (including Mexico and Canada), AMTRAK and most public transit providers servicing the major population centers in the United States, key railroad customers (such as chemical companies and car manufacturers), and others.

Development of Strategies, Guidance, and Standards for Improving Security

As part of their efforts to improve the security posture of their respective sectors, sector representatives have developed strategies and other guidance to drive their sector-wide activities and assist individual entities. Several sectors, including financial services, electricity, oil and gas, the rail segment of the transportation sector, information and telecommunications, water, and chemical, have developed strategies that outline priorities and efforts for the sector that were part of the efforts to develop *The National Strategy to Secure Cyberspace*. These strategies address subjects, such as increasing the awareness of senior officials, encouraging greater participation in sector activities, and identifying and reducing vulnerabilities. For example, we reported in January 2003[29] that financial services industry representatives collaborated on a Treasury-sponsored working group to develop the sector's *National Strategy for Critical Infrastructure Assurance*, which was issued in May 2002.[30] In addition, one of the five key elements of the chemical sector's cybersecurity strategy involves the establishment of management practices, procedures, guidelines, and standards to support overall sector cybersecurity.

As we have previously described, there have also been efforts in the energy and chemical sectors to provide greater specificity with regard to the elements in the strategies and to provide guidance and standards. For example, in January 2003, the Chemical Industry Data Exchange (CIDX)[31] established the Chemical Sector Cybersecurity Practices, Standards, and Technology Initiative to address two elements of the chemical sector cybersecurity strategy: (1) establishing sector cybersecurity practices and standards by working with the American Chemistry Council's Responsible

[29]U.S. General Accounting Office, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, GAO-03-173 (Washington, D.C.: Jan. 30, 2003).

[30]Banking and Finance Sector, *Defending America's Cyberspace*.

[31]CIDX is a trade association and standards body focused on improving the ease, speed, and cost of transacting business electronically between chemical companies and their trading partners.

Care Security Code program,[32] and (2) accelerating development of improved security technology and solutions by bringing technology solution providers to the table with chemical sector information technology and process control system experts to improve technology security. According to chemical infrastructure sector officials, during the second quarter of 2003, CIDX released its first work products, including cybersecurity guidance for the Responsible Care Security Code, cybersecurity guidance for security vulnerability assessment methodology, and the results of baseline assessments against the ISO 17799 standard for security management practices.

The energy infrastructure sector has also taken steps to develop guidance and standards. For example, NERC has developed minimum security requirements to govern the exchange of electronic information needed to support grid reliability and market operations.[33] In addition, the oil and natural gas segment of the energy infrastructure sector has security guidelines available that include guidance on cybersecurity.[34] The guidance provides a means to improve the security of the oil and gas industry from cyber terrorism and to effectively allocate resources. It also endorses the use of ISO/IEC International Standard 17799 on information security management as a voluntary framework to protect the industry against cyber terrorism.

Providing Methods for the Independent Validation of Software and Hardware

Infrastructure sectors have recognized the need to improve the ability of individual entities to understand the level of security offered by the technology products they use and the risks of using those technologies. For example, as we reported in January 2003, BITS provides for the financial services sector through the BITS Product Certification

[32]The Responsible Care initiative, now in its 14th year, is a comprehensive management system developed by experts for use throughout the chemical sector to continuously improve safety performance and communications and to protect employees, communities, and the environment. Members of sector associations, such as the American Chemistry Council and the Synthetic Organic Chemical Manufacturers Association, along with other companies and associations involved in the sector's supply chain, participate in Responsible Care as partners. As a result, hundreds of companies are working together to further improve safety and performance throughout commerce and communities.

[33]The North American Electric Reliability Council, *The North American Electric Reliability Council's Urgent Action Standard 1200—Cyber Security*, adopted by NERC Board of Trustees August 13, 2003.

[34]American Petroleum Institute, *Security Guidelines for the Petroleum Industry*, Second Edition (Washington, D.C.: Apr. 2003).

Program—designed to test products against baseline security criteria—a vehicle to significantly enhance safety and soundness by improving the security of technology products and reducing technology risk.[35] In addition, as one of its key elements, the chemical sector cybersecurity strategy included the acceleration of the development of cost-effective technology solutions by proactively working with service providers, government, and academia.

Raising Awareness about the Importance of Cybersecurity

An important aspect of improving the cybersecurity of an entity is raising the awareness of senior executives and others about the risks their entities face because of their reliance on IT and the importance of appropriately protecting those assets and the related information. For example, the financial services sector's efforts are designed to increase the awareness of officials within the sector about the importance of cybersecurity. In addition, the financial services sector's strategy addresses actions to educate industry executives and information security specialists.

Encouraging the Performance of Vulnerability Assessments

As discussed earlier, the most recent federal CIP policy, HSPD-7, requires sector-specific agencies to conduct or facilitate vulnerability assessments of their respective sectors, which is a continued emphasis on performing such assessments. To address the need for vulnerability assessments, some sectors have taken steps to perform sector-wide vulnerability assessments or encourage or require individual entities to perform vulnerability assessments for their facilities and operations. For example, following the September 11, 2001 terrorist attacks, the railroad industry established five critical action teams, including an information technology and communications team, to assess both short-term and long-term security needs. The teams, with assistance from outside experts, evaluated threats to the rail system, identified vulnerabilities, quantified risks, and devised appropriate countermeasures. As a result of the team's efforts, a railroad security plan was developed that identifies industry action and government support required to enhance the security of the freight rail industry, including the need to cooperate to meet the security and redundancy requirements for critical data communications and train

[35]BITS is the name of the Technology Group for The Financial Services Roundtable. As part of its mandate, BITS strives to sustain consumer confidence and trust by ensuring the safety and security of financial transactions, and it has several initiatives under way to promote improved information security within the financial services industry. BITS's and the Roundtable's membership represents 100 of the largest integrated financial services institutions providing banking, insurance, and investment products and services to American consumers and corporate customers.

control systems. Further, the chemical sector cybersecurity strategy has as one of its key elements identifying and reducing infrastructure vulnerabilities to guard against cyber attacks and speed recovery from incidents. Also, as one of its current focuses, CIDX has taken steps to develop a cybersecurity risk management process and framework, participate in the development of process control standards and technical reports that provide preliminary security recommendations, and develop requirements for manufacturing process controls. The financial services sector strategy also identifies a framework for sector actions that presents efforts necessary to identify, assess, and respond to sector-wide threats, including completion of a sector-wide vulnerability assessment.

Some infrastructure entities have also conducted vulnerability assessments. For example, entities in the chemical sector that are required to follow the Responsible Care Security Code perform security vulnerability assessments by prioritizing their sites. Entities are also to conduct assessments of their value chain and cyber networks. In addition, according to chemical sector representatives, there are efforts under way to partner with other institutions, including Sandia National Laboratories, to develop a more robust cybersecurity vulnerability assessment methodology. Together with Sandia Laboratories and the Center for Chemical Processing Safety, CIDX has submitted to DHS a request for funding to develop a combined cyber and physical vulnerability assessment methodology for use in site vulnerability assessments. Industry representatives at the time of our study also stated that 14 chemical companies had conducted an assessment of their company's performance against ISO 17799. Also, according to defense industrial base representatives, individual companies continually perform security assessments.

Sharing CIP-Related Activity Information across Sectors

Individual sectors share information with other sectors because they use the same technology and thus face the same security challenges and are interdependent on each other. For example, to encourage cross-sector coordination and information sharing, the ISAC Council was formed by several ISACs to advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government. Currently, the participating ISACs include Chemical, Electricity, Energy, Financial Services, Highway, Information Technology, Public Transit, Surface Transportation, Telecommunications, and Water. In addition, the Multi-state and Research and Education Networking ISACs are participants.

The Council has met with DHS to discuss mutual expectations. According to one infrastructure sector official, the ISAC Council has resulted in better communications among the various ISACs, and they have begun to help each other to establish and maintain a policy for inter-ISAC coordination, a dialogue with governmental agencies that deal with ISACs, and a practical data and information-sharing protocol. In February 2004, the council issued eight white papers to reflect the collective analysis of its members and to cover a broad set of issues and challenges, including government/private sector relations, information sharing and analysis, ISAC analytical efforts, policy and framework for the ISAC community, and the reach of major ISACs.

Sharing Best Practices

As part of their efforts to share information, sectors have established methods for individual entities to share best practices across the sector. For example, NERC has created best practices for protecting critical facilities against physical and cyber threats. In addition, one of FSSCC's goals is to identify, develop, and share industry best practices to maximize sector resiliency. Also within the financial services sector, BITS actively seeks information security improvements, including issuing a framework of industry practices and regulatory requirements for managing technology risk for IT service provider relationships.

Leveraging Existing Efforts

To address CIP issues within their respective sectors, some sectors have attempted to use existing efforts to enhance the level of awareness and action and minimize the risk of duplicative efforts. For example, in the financial services sector, one of the main initiatives of the FSSCC is to share information on CIP activities that are already being performed by member associations across the entire sector. For example, the American Bankers Association (ABA) and BITS have a number of initiatives to improve the cybersecurity of the sector.[36] In addition, according to industry representatives, the Chemical Sector Cybersecurity Program is leveraging proven sector initiatives, including chemical trade associations (through the Chemical Sector Cybersecurity Information Sharing Forum), CIDX, and the Chemical Sector ISAC.

[36]ABA is an industry group whose membership includes community, savings, regional, and money center banks; savings associations; trust companies; and diversified financial holding companies.

Federal Government Actions to Improve Cybersecurity for CIP

As we have described, the federal government has several ongoing activities designed to improve the cybersecurity posture of critical infrastructures. There is a variety of ways in which the federal government could encourage the use of cybersecurity technologies for critical infrastructure protection. Besides merely continuing the current programs, the federal government could choose to expand current programs or develop new programs to assist critical infrastructures. The design of federal policy will play a vital role in determining success and ensuring that national goals are met. Key to the national effort will be determining the appropriate level of funding, so that policies and tools can be designed and targeted to elicit a prompt, adequate, and sustainable response while also protecting against federal funds being used to substitute for spending that would occur anyway.

As with any policy decision, there are a number of factors that should be considered before selecting an approach. First, the problem needs to be identified. There is a need for factual information on the scope and scale of the cyber vulnerabilities and the consequences of possible cyber attacks on the critical infrastructure. The technology issues surrounding the problem and the structure of the security marketplace have to be determined. Although experts agree that cybersecurity is an important element of critical infrastructure protection, the scope and scale of the problem and the consequences of cyber attacks are not easily quantifiable.

As we have described, because about 85 percent of the critical infrastructure is owned by the private sector, the federal government cannot act alone to protect it. To help determine the proper approach for federal action, the government will require information from the private sector on the scope and size of the cybersecurity risks and the actions that they are already taking to address them. To make informed decisions on cybersecurity policy, federal policy makers need information on critical infrastructure assets, vulnerabilities, and priorities from the private sector, information that could be gleaned if the risk-based framework for security that we have described is followed.

After the parameters of the problem have been established, possible private and public responses can be proposed. To interact with the private sector, the federal government can use a variety of policy options to motivate or mandate private sector entities to take actions to address cybersecurity concerns. These options include grants, regulations, tax incentives, and coordination and partnerships.

Two key considerations in developing a grant program are targeting the funds to those with the greatest need and striking a balance between accountability and flexibility. Accountability can be established for measured results and outcomes that permit greater flexibility in how funds are used while at the same time ensuring some national oversight. An example of a grant program would be one where the federal government funds or subsidizes the purchase of security technology for specific critical infrastructure sectors or specific groups of vulnerable entities within a sector. There is precedent for this in the Help America Vote Act of 2002, which provides funding to states for buying new voting machines.[37] Another example is the Environmental Protection Agency, which reported providing 449 grants to assist large drinking water utilities in developing vulnerability assessments, emergency response/operating plans, security enhancement plans and designs, or a combination of these efforts.

In designing regulations, key considerations include determining how to provide federal protections, guarantees, or benefits while preserving an appropriate balance between the federal government and state and local government and between the public and private sectors. In designing a regulatory approach, one of the challenges is determining who will set the standards and who will implement or enforce them.

Tax incentives are the result of special exclusions, exemptions, deductions, credits, deferrals, or tax rates in the federal tax laws. Unlike grants, tax incentives do not generally permit the same degree of federal oversight and targeting, and they generally are available to all potential beneficiaries who satisfy congressionally established criteria. However, according to some infrastructure sector officials, tax incentives will not provide adequate motivation to organizations that are already under financial strain or under bankruptcy protection.

Sometimes the federal government can make change happen in a sector by requiring that sector to work in a certain way when it interacts with government systems. An example is the Department of the Treasury directive that required electronic funds transfer transactions involving federal systems to use DES encryption. Similarly, to promote adoption of more secure products and practices, specific sector systems that connect to government systems could be required to meet specific cybersecurity provisions. The key is for government and the sector to decide what types

[37]Help America Vote Act of 2002, Public Law 107-252 (Oct. 29, 2002).

of cybersecurity requirements to adopt and to understand why these requirements improve security.

The government owns approximately 15 percent of the critical infrastructure and is otherwise a major purchaser of information technology. Consequently, it could affect market behavior through its own purchases. For instance, government could promulgate procurement rules specifying that after a certain number of years it will no longer buy PCs without certain security features built into the hardware and operating system. For example, currently all cryptography products purchased by the federal government must be compliant with FIPS 140-2.

Critical infrastructure protection is a complex mission that requires high levels of interagency, interjurisdictional, and interorganizational cooperation. Different levels of government—federal, state, and local—as well as various public, private, and nongovernmental organizations are involved with CIP. Promoting partnerships among these different organizations facilitates the maximizing of resources and supports coordination.

Without appropriate consideration of public policy tools, private sector participation in sector-related information sharing and other CIP efforts may not reach its full potential. For example, in January 2003, we reported on the efforts of the financial services sector to address cyber threats, including industry efforts to share information and to better foster and facilitate sector-wide efforts.[38] We also reported on the efforts of federal agencies and regulators to partner with the financial services industry to protect critical infrastructures and to address information security. We found that although federal agencies had a number of efforts ongoing, the Treasury Department, in its role as sector liaison, had not undertaken a comprehensive assessment of the potential public policy tools that could be used to encourage the financial services sector in implementing information sharing and other CIP-related efforts. Since then, Treasury provided $2 million to help establish the next generation FS-ISAC and its new capabilities, including improving information sharing by upgrading the technology supporting the FS-ISAC and adding information about physical threats to the cyber threat information it disseminates.

[38] GAO-03-173.

In addition, in February 2003, we reported on the mixed progress that the telecommunications, electricity, information technology, energy, and water sectors had made in accomplishing the activities suggested by Presidential Decision Directive 63 (PDD 63).[39] We found that the responsible lead agencies needed to better assess the need for public policy tools to encourage increased private sector CIP activities and facilitate greater sharing of intelligence and incident information between the sectors and the federal government.

Considerations for Federal Action

For each possible policy option, it is necessary to analyze the costs and benefits, how the policy can be implemented, and the consequences of action and inaction. Because resources are scarce, decisions on spending must achieve two overarching goals: to devote the right amount of resources to cybersecurity and to spend those resources on the right activities. To achieve the first goal, the benefit of each endeavor must be carefully weighed, and resources should only be allocated where the benefit of reducing risk is worth the amount of additional cost.

One of the essential parts of any federal program is the ability to measure the results from the program. However, the lack of well-defined security standards or benchmarks makes it difficult to measure the benefit of a security program. Further, what may be appropriate for some sectors may not be appropriate for other sectors. For policy options such as grants, tax incentives, and regulations, there needs to be a way of defining the actions or the outcomes that are being sought by the federal government. Instead of requiring a set of actions, it is best to aim for specific outcomes. A problem with this approach is that sometimes it is not possible to specify a measurable outcome. In the absence of such criteria, it will be challenging to define and implement such a federal program.

For example, to use grants for the purchase of cybersecurity technology or to impose requirements for government purchases, the government needs to work with the sectors and the technology vendors to set standards for cybersecurity products or establish measurable outcomes to be achieved by the technology. Unfortunately, it is difficult to set product-level standards that can be evaluated efficiently and without incurring significant additional cost.

[39]U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, D.C.: Feb. 28, 2003).

The federal government has several ongoing cybersecurity programs. For example, the federal government has previously assisted sectors with conducting risk assessments, provided threat and vulnerability information to sectors and their entities, and established education and awareness programs on cybersecurity. To assist with the costs and benefits determination of future programs, it would be useful to examine the effectiveness of existing programs.

One possibility is to measure the costs saved by preventing a cyber attack. According to *The National Strategy to Secure Cyberspace*, surveys have repeatedly shown that although the likelihood of suffering a severe cyber attack is difficult to measure, the costs associated with mitigating and reconstituting after a successful attack are likely to be greater than the investment in a cybersecurity program to prevent it. Financial losses resulting from worms and viruses have been significant. PricewaterhouseCoopers estimated that in 2001, hackers, worms, and viruses caused almost $1.6 trillion in downtime and recovery costs. Table 12 shows the estimated costs of recent notable computer attacks.

Table 12: Estimated Costs of Recent Worm and Virus Attacks

Incident	Date	Estimated cost
Melissa	1999	$0.3 billion
I Love You	2000	$8.0 billion
Code Red	2001	$2.6 billion
Slammer	2003	$1.0 billion

Source: Canadian Office of Critical Infrastructure Protection and Emergency Preparedness.

It is important to consider the proper role of the federal government. Sometimes, the best course of action may be to take no action at all. The federal government can take action because a particular activity is best performed at a national or sub-national level. For example, intelligence gathering and national defense are best accomplished by the federal government. On the other hand, while the costs of recovering from cyber attacks can be high, some have argued that the potential effect of cyber attacks on national security or public safety is relatively small. It is argued that many critical infrastructure sectors are more robust and resilient than generally believed. For example, during the October 2002 distributed denial-of-service attack on the Domain Name Server root servers, 8 of the 13 servers were forced off-line. However, the attack did not noticeably degrade Internet performance. Similarly, while thousands of networks

were disabled during the August 2003 northeast blackout, there was no significant increase in end-to-end delays on the Internet.

In other situations, the federal government may need to take action because the market will not address the issue in a timely fashion. Ideally, private sector responses will adequately address a problem. In some sectors, market forces may be enough to improve cybersecurity throughout the sector. Some well-organized sectors could also develop their own rules requiring all member entities to achieve specific cybersecurity results. For example, the chemical infrastructure sector established mandatory requirements under its responsible care program. As previously discussed, the oil and natural gas industry also endorsed international standards for security management programs. In other cases, state and local government may be taking action to address the problem. Regardless of the specific actions taken by the federal government, it is important for all levels of government—federal, state, and local—and the private sector to work cooperatively to ensure that the most critical issues are addressed by the appropriate party.

The Federal Government Is Assisting with Risk Assessments

The federal government has a direct interest in ensuring that the private sector is adequately protecting critical infrastructures. To assist with the critical infrastructure risk assessment process, the federal government provides two primary functions: (1) it provides guidance and establishes relationships to help conduct risk assessments, and (2) it provides threat and vulnerability information to sectors and their member entities.

HSPD-7 and the *National Strategy for Homeland Security* identified lead federal agencies, referred to as sector-specific agencies, to work with their counterparts in the private sector, referred to as sector coordinators. HSPD-7 called for a range of activities intended to establish a partnership between the public and private sectors to ensure the security of our nation's critical infrastructures. The sector-specific agency and the sector coordinator are to work with each other to address problems related to CIP for their sector. In particular, HSPD-7 stated that they are to (1) conduct or facilitate vulnerability assessment of their sector, and (2) encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructures and key resources. It also required federal agencies to establish a system for responding to a significant attack on an infrastructure while it is under way so that damages can be isolated and minimized and for rapidly reconstituting minimum required capabilities for varying levels of successful infrastructure attacks.

The National Strategy for Homeland Security and HSPD-7 identified 13 industry sectors, expanded from the 8 originally identified in PDD 63, and lead federal agencies, including the Department of Homeland Security. The lead agencies and their corresponding sectors are listed in table 13.

Table 13: Critical Infrastructure Sector-Specific Agencies

Sector-specific agency	Sectors
Department of Agriculture	• Agriculture • Food (meat and poultry)
Department of Defense	• Defense industrial base
Department of Energy	• Energy (electrical power, oil and gas production and storage)
Environmental Protection Agency	• Drinking water and water treatment systems
Department of Health and Human Services	• Public health (including prevention, surveillance, laboratory services, and personal health services) and health care • Food (all except meat and poultry)
Department of Homeland Security	• Chemicals and hazardous materials • Continuity of government • Emergency services • Information technology and telecommunications • Transportation (aviation; rail; mass transit; waterborne commerce; pipelines; and highways, including trucking and intelligent transportation systems) • Postal and shipping
Department of the Treasury	• Banking and finance

Source: *National Strategy for Homeland Security*, *The National Strategy to Secure Cyberspace*, and HSPD-7.

For example, as part of its responsibilities as the lead agency for the banking and finance infrastructure sector, the Department of the Treasury chairs the Financial and Banking Information Infrastructure Committee (FBIIC), which is responsible for coordinating federal and state regulatory efforts to improve the reliability and security of U.S. financial systems. Treasury has taken steps designed to establish better relationships and methods of communication among regulators, assess vulnerabilities, and improve communication within the financial services sector. In addition, federal regulators, such as the Federal Reserve System and the Securities and Exchange Commission, have taken several steps to address information security issues, including the consideration of information security risks in determining the scope of their examinations of financial

institutions and the development of guidance for examining information security and for protecting against cyber threats.

Further, the federal government can also help fund risk assessment activities by sectors and their member entities. This support can be provided directly to infrastructure owners or through their ISACs or sector coordinators. There is already precedence for such support. For example, as mentioned earlier, the Environmental Protection Agency reportedly has provided funding for 449 grants totaling $51 million to assist utilities for large drinking water systems in preparing vulnerability assessments, emergency response/operating plans, and security enhancement plans and designs. In addition, the Department of Transportation has performed related studies, including a vulnerability assessment of surface transportation and of the transportation infrastructure's reliance on the global positioning system.[40] The Department of the Treasury provided $2 million for the next generation Financial Services ISAC to provide alerting services to a greater number of sector entities.

Additionally, the federal government could provide guidance to critical infrastructure owners on how to perform risk assessments. Such guidance could be in the form of risk assessment templates that cover key elements such as threat and vulnerability assessments.

The federal government also provides assistance by disseminating threat and vulnerability information to critical infrastructure sectors. DHS is responsible for analyzing terrorist threats to the homeland, mapping these threats to our vulnerabilities, and taking protective action. For example, DHS administers the Homeland Security Advisory System, including coordination with other federal agencies to provide specific warning information and advice to state and local agencies, the private sector, the public, and other entities about appropriate protective measures and countermeasures to homeland security threats.

In March 2003, DHS assumed many of the functions of NIPC from the FBI. DHS's IAIP directorate provides a focal point for gathering and disseminating information on threats to critical infrastructures and issues warning products in response to increases in threat condition. The

[40]John A. Volpe National Transportation Systems Center, *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*, Final Report (Cambridge, MA: Aug. 29, 2001).

Homeland Security Act gives DHS broad statutory authority to access intelligence information, as well as other information relevant to the terrorist threat, and to turn this information into useful warnings. For example, DHS is one of the partner organizations in the multi-agency Terrorist Threat Integration Center (TTIC), which began operations on May 1, 2003.[41] IAIP integrates all-source threat information and analysis that it receives from TTIC and other agencies with its own vulnerability assessments to provide tailored threat assessments.

The United States Computer Emergency Readiness Team, a partnership between DHS and the private sector, issues a variety of information products through its National Cyber Alert System. This system distributes three types of information products: (1) cybersecurity alerts, which are available for non-technical and technical audiences, provide real-time information about security issues, vulnerabilities, and exploits current occurring that could require rapid action; (2) cybersecurity bulletins are targeted at technical audiences and provide biweekly summaries of security issues, new vulnerabilities, potential effect, patches, and workarounds; and (3) cybersecurity tips are targeted at non-technical audiences and provide biweekly information on best computer security practices. According to IAIP officials, if it is necessary to relay classified material, secure communication links have been established with each of the 50 state homeland security offices and some of the ISACs. Once it is determined that information should be disseminated, it is sent out by multiple paths. The difficult task is determining the appropriate audience for the information. The interdependency among the infrastructures is one reason why it is difficult to determine the appropriate audience.

A National CIP Plan Can Help Prioritize Needs

The scope of any federal program must account for the wide breadth of critical infrastructure sectors. However, the assets, functions, and systems within each critical infrastructure sector are not equally important. For example, the transportation sector is vital, but not every bridge is critical to the nation as a whole. To ensure a comprehensive and well-coordinated approach to critical infrastructure protection across all organizations, we

[41]The center was formed from elements of the FBI, the CIA, and the Departments of Defense, Homeland Security, and State.

have previously reported on the need for a national CIP plan.[42] Such a plan should clearly define the roles and responsibilities of federal and nonfederal CIP organizations, define objectives and milestones, set time frames for achieving objectives, and establish performance measures. The federal government could then use this plan as a framework to help it determine the appropriate amount and types of federal actions that would best protect critical infrastructures from attack.

The need for a coordinated plan results from the widely varying operations of the critical infrastructure sectors and the sheer number of organizations that are involved in CIP efforts. For example, in 2002, we reported that at least 50 federal organizations were involved in national or multinational cyber CIP efforts, including 5 advisory committees; 6 Executive Office of the President organizations; 38 executive branch organizations associated with departments, agencies, or intelligence organizations; and 3 other organizations.[43] In addition, there are many state and local government agencies involved in CIP efforts, such as state regulators, law enforcement agencies, and water authorities, as well as private sector organizations, such as trade associations, industry groups, corporations, and information sharing and analysis centers. While each sector can take a sector-wide look and entities can focus on the details of the infrastructure they own, the federal government is in a better position to look across all critical infrastructure sectors and conduct a risk-based identification of the truly critical infrastructures—assets whose destruction or incapacitation would have a debilitating impact on national security, the economy, or public health and safety. Because such a large number of organizations are involved in CIP efforts, it is necessary to clarify how these organizations coordinate their activities with each other.

As we have described, several federal CIP policy documents have identified the need for such a plan. *The National Strategy for Homeland Security* assigns the development of a national infrastructure protection plan to the Department of Homeland Security. The Homeland Security Act

[42]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, D.C.: Sept. 20, 2001); and *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, GAO-02-474 (Washington, D.C.: July 15, 2002).

[43]GAO-02-474.

of 2002 further assigns this responsibility to the IAIP directorate.[44] Most recently, HSPD-7 requires that this plan be developed by December 2004 and states that it should include a strategy to identify, prioritize, and coordinate the protection of critical infrastructure. Nationwide critical infrastructure risk assessments could enable the federal government to develop and maintain a prioritized list of key infrastructures across sectors. Knowing which infrastructures are truly critical across all sectors can help the government apply limited resources where they are most needed. This plan is expected to inform DHS's annual process for planning, programming, and budgeting critical infrastructure protection activities, including research and development.

However, the development of such a plan is not without its challenges. For instance, methodologies to prioritize efforts to enhance critical infrastructure protection are inconsistent. Further, in order to properly define roles and responsibilities for critical infrastructure organizations, it is necessary to overcome ineffective communication among the federal, state, and local governments, which has resulted in untimely, disparate, and at times conflicting communication.

Increasing the Use of Available Cybersecurity Technologies

While many cybersecurity technologies are available, experts believe that these technologies are not being purchased or implemented to their fullest extent. Besides providing funding for the purchase of technology by critical infrastructure owners, other methods have been suggested to increase the use of available cybersecurity technologies, including increasing the security awareness of system administrators and users and enhancing information sharing so that security vulnerabilities can be better understood.

Improving Cybersecurity Awareness

As computers are increasingly interconnected and achieve appliance status, they are no longer strictly the domain of technology-savvy workers. According to CERT/CC, the expertise of the average system administrator continues to decline. A larger number of systems that are connected to the Internet are administered and used by individuals with little or no security training or expertise. Many experts agree that there is a need to improve cybersecurity awareness at all user levels, even for business and home users, because any Internet-connected PC could be used as a launching pad for denial-of-service attacks. Users often are unaware that their computers have been compromised and are being used to launch attacks.

[44]Public Law 107-296, §201(d)(5).

Even among those who are familiar with cybersecurity technologies such as firewalls, encryption, and antivirus software, users do not always implement these security-improving technologies to their fullest extent. Some say that users often are complacent about possible cyber threats or do not adequately maintain the security posture of their systems by implementing security patches on a timely basis. Others say that users simply cannot keep up with the constant stream of software patches that are needed to correct defects in software.

The federal government could take the lead in promoting cybersecurity awareness as it has done in other awareness campaigns such as the campaign to discourage illicit drug use and the Buckle Up America campaign, which promotes automobile seat belt use. The federal government can fund the development of education campaigns that teach the importance of cybersecurity and how to use information technology securely.

Educational institutions could incorporate cybersecurity and cyberethics education in primary and secondary school and in colleges. The Department of Justice has established a Cyberethics for Kids program that teaches students in elementary and middle schools about the risks of harmful and illegal behavior online and shows them how to protect themselves from such behavior. For university students, NSF funds the Federal Cyber Service program to increase the number of qualified students in the cybersecurity field and to increase the number of cybersecurity professionals. The Federal Cyber Service program has two tracks: a Scholarship Track and a Capacity Building Track. The Scholarship Track provides funding to colleges and universities to award scholarships in information assurance and computer security fields. Upon graduation, after their 2-year scholarships, the scholarship recipients are required to work for a federal agency for 2 years in fulfillment of their Federal Cyber Service commitment. The Capacity Building Track provides funds to colleges and universities for professional development of information assurance faculty and the development of academic programs.

Some experts also commented that all business managers should learn the basics of cybersecurity—why it is important to the business and how to include it in risk analyses. Even if a business does not deal with life-and-death systems, managers need to know that cybersecurity helps protect against industrial espionage that could be used to steal sensitive information such as business plans, creative ideas, and trade secrets.

Critical infrastructure sectors could conduct their own security awareness campaigns. For example, the Federal Deposit Insurance Corporation (FDIC) has sponsored regional information sessions for the FBIIC and FSSCC to inform financial services organizations about the importance of a public-private sector partnership and to raise awareness of the services available to those organizations that are provided by the federal government and by the financial services sector.

Some experts have stated that one of the causes of vulnerable computers is a lack of awareness by users and system administrators in keeping up with available security patches. To remedy this problem, various tools and services are available to assist them in identifying vulnerabilities and their respective patches.

Because it can be difficult to identify vulnerabilities, the use of multiple sources can help to provide a more comprehensive view. As we have described, there are several sources of vulnerability information, including CERT/CC and NIST's ICAT Metabase. ICAT links users to publicly available vulnerability databases and patch sites, thus enabling them to find and fix vulnerabilities on their systems. Other organizations, such as the Last Stage of Delirium Research Group, research security vulnerabilities and maintain databases of such vulnerabilities. In addition, mailing lists, such as BugTraq, provide forums for announcing and discussing vulnerabilities, including information on how to fix them. Security Focus monitors thousands of products in order to maintain a vulnerability database and provide security alerts. Finally, vendors such as Microsoft and Cisco provide software updates on their products, including notices of known vulnerabilities and their corresponding patches.

Several services and automated tools are available to assist organizations in performing their patch management function, including tools designed as stand-alone patch management systems. In addition, systems management tools can be used to deploy patches across an organization's network. Patch management vendors also offer central databases of the latest patches, incidents, and methods for mitigating risks before a patch can be deployed or before a patch has been released. Some vendors provide support for multiple software platforms, such as Microsoft, Solaris, Linux, and other platforms, while other vendors, such as Microsoft, focus on certain platforms exclusively.

Enhancing Information Sharing

Information sharing is a key element in developing comprehensive and practical approaches to defending against cyber attacks that could threaten critical infrastructures. Sharing of vulnerability or threat

information with infrastructure owners facilitates the prevention or detection of cyber attacks. However, as we have reported in recent years, establishing the trusted relationships and protocols necessary to support information sharing can be difficult.[45] In addition, the private sector has expressed concerns about sharing information with the government and about the difficulty of obtaining security clearances.

Critical infrastructure sectors can benefit from sharing information about vulnerabilities, threats, and details of cyber attacks among the entities that make up the sector. Information on threats, vulnerabilities, and incidents experienced by others can help to identify trends, better understand the risks they faced, and determine what preventive measures should be implemented. However, for such information sharing to work, it is necessary to develop fully productive information-sharing relationships within the federal government and between the federal government and state and local governments and the private sector.

Shared information could be used for tactical purposes. Sharing information on incidents and solutions during an attack can lead to better responses by all involved in the information-sharing arrangement. Such a structure could be used to contain and minimize the damage caused by cyber attacks. Shared information can also have strategic uses. Computer security experts and researchers can use historical data about attacks to better understand threats and vulnerabilities and to develop better technologies that can defend against similar attacks. Further, analysis of such information can help intelligence and law enforcement organizations to identify trends in attacks and potentially to identify the perpetrators of attacks or sources of future attacks.

We have previously reported on federal information sharing practices that could benefit CIP.[46] These practices include:

- establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;

[45]U.S. General Accounting Office, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

[46]GAO-02-24, 18.

- developing standards and agreements on how shared information will be used and protected;
- establishing effective and appropriately secure communications mechanisms; and
- taking steps to ensure that sensitive information is not inappropriately disseminated, steps that may require statutory changes.

A number of activities have been undertaken to build relationships between the federal government and the private sector, such as InfraGard, the Partnership for Critical Infrastructure Security, efforts by the former Critical Infrastructure Assurance Office, and efforts by lead agencies to establish ISACs. For example, the InfraGard Program, which provides the FBI with a means for sharing information securely with individual companies, has expanded substantially. Members include representatives from private industry, other government agencies, state and local law enforcement, and the academic community. As of March 30, 2004, InfraGard members totaled over 11,000.

PDD 63 encouraged the voluntary creation of ISACs and suggested some possible activities. However, their actual design and functions were left to the private sector, along with their relationships with the federal government. HSPD-7 continues to encourage the development of information-sharing mechanisms and does not suggest specific ISAC activities. As a result, the ISACs have been designed to perform their missions based on the unique characteristics and needs of their individual sectors, and although their overall missions are similar, they have different characteristics. They were created to provide an information-sharing and analysis capability for members of their respective infrastructure sectors in order to support efforts to mitigate risk and provide effective response to adverse events, including cyber, physical, and natural events.

As previously discussed, Treasury provided $2 million to establish the next generation FS-ISAC and its new capabilities, including upgrading the technology supporting it that would benefit Treasury, other financial regulators, and the private sector. In announcing this contract in December 2003, Treasury reported that it would:

- Transform FS-ISAC from a technology platform that serves approximately 80 financial institutions to one that serves the entire 30,000 institution financial sector including banks, credit unions, securities firms, insurance companies, commodity futures merchants, exchanges, and others.

- Provide a secure, confidential forum for financial institutions to share information among one another as they respond in real-time to particular threats.
- Add information about physical threats to the cyber threat information that FS-ISAC currently disseminates.
- Include an advance notification service that will notify member financial institutions of threats. The primary means of notification will be the Internet. If, however, Internet traffic is disrupted, the notification will be by other means, including telephone calls and faxes.
- Include over 16 quantitative measures of FS-ISAC's effectiveness that will enable the leadership of FS-ISAC and Treasury to assess both the FS-ISAC's performance and the aggregate state of information sharing within the industry in response to particular threats.

Laws recently enacted by Congress and the administration strengthen information sharing. For example, the USA PATRIOT Act promotes information sharing among federal agencies, and numerous terrorism task forces have been established to coordinate investigations and improve communications among federal and local law enforcement agencies.[47] Moreover, the Homeland Security Act of 2002 includes provisions that restrict federal, state, and local government use and disclosure of critical infrastructure information that has been voluntarily submitted to DHS.[48] These restrictions include exemption from disclosure under FOIA, a general limitation on use to CIP purposes, and limitations on use in civil actions and by state or local governments. The act also specifies penalties for any federal employee who improperly discloses any protected critical infrastructure information.

Nonetheless, some in the private sector have expressed concerns about voluntarily sharing information with one another and with the federal government. Specifically, concerns have been raised that sector members could face antitrust violations for sharing information with other industry partners, have their information subject to the Freedom of Information Act

[47]The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (Public Law 107-56, Oct. 26, 2001).

[48]Public Law 107-296, §§211-215.

(FOIA),[49] or face potential liability concerns for information shared in good faith. For example, the information technology, energy, and water ISACs do not share their libraries with the federal government because of concerns that information could be released under FOIA. Officials of the energy ISAC stated that they had not reported incidents to NIPC because of FOIA and antitrust concerns.

Developing New Cybersecurity Technology

While there is clearly a short-term need for cybersecurity solutions, many researchers have described this approach as short-sighted. Because new vulnerabilities are being discovered on an increasingly frequent basis, many have argued that what is required is a re-engineering of security. Researchers have argued that there is a need to design secure systems from the bottom up, because it is difficult to deploy secure systems based on insecure components. Longer-term efforts, such as research into cybersecurity vulnerabilities and technological solutions for those problems and the transition of research results into commercially available products, are needed.

Continuing Cybersecurity Technology Research

Research in cybersecurity technology is needed to create a broader range of choices and more robust tools for building trustworthy networked computer systems. Research provides a science base and engineering expertise for building secure systems. Because research takes time to produce results, it is important to initiate research soon.

The federal government supports cybersecurity research, primarily through the Defense Advanced Research Projects Agency (DARPA) and NSA, but also through other Department of Defense and civilian agencies, such as NSF and DHS. There is also industry-funded research and development in the area of information security, but that work typically emphasizes development over research. It is difficult to enumerate all federally funded cybersecurity research because of problems in understanding how different projects are accounted for and also because many projects are classified. Additionally, research in cybersecurity may include system development activities. For example, some recent research projects involve building network testbeds to develop and test defenses against cyber attacks. Two recent examples are the jointly NSF- and DHS-funded Cyber Defense Technology Experimental Research network, or DETER, at the University of California at Berkeley and the University of Southern California, and the Department of Justice-funded Internet-Scale

[49] 5 U.S.C. §552.

Event and Attack Generation Environment at Iowa State University. Such test bed projects include the cost of the network itself in the project costs.

Because research is often geared toward producing short-term results and rapid transition to industry, high-risk theoretical and experimental investigations are not always encouraged. Many research problems are difficult, and the focus on short-term results can divert effort from critical areas.

A number of recent publications provide cybersecurity research agendas with varying degrees of detail.[50] These research agendas have similarities with one another. While several research agendas have been produced, some researchers have commented that insufficient action has been taken to implement them. Table 14 summarizes the typical research topics from a number of agendas.

[50]Some of these sources of research agendas include (1) Institute for Information Infrastructure Protection (I3P), *Cyber Security Research and Development Agenda* (Jan. 2003); (2) INFOSEC Research Council, *Information Assurance R&D Strategy: National Needs and Research Programs* (July 2, 2002); (3) NSF/OSTP, *New Vistas in CIP Research and Development: Secure Network Embedded Systems, Report of the NSF/OSTP Workshop on Innovative Information Technologies for Critical Infrastructure Protection* (Sept. 19-20, 2002); (4) National Security Telecommunications Advisory Committee (NSTAC), *Research and Development Exchange Proceedings: Research and Development Issues to Ensure Trustworthiness in Telecommunications and Information Systems That Directly or Indirectly Impact National Security and Emergency Preparedness* (Mar. 13-14, 2003); and (5) National Research Council, *Trust in Cyberspace* (Washington, D.C.: National Academy Press, 1999).

Table 14: Typical Research Areas Identified in Research Agendas

Research area	Description
Building secure systems from insecure components	Biological metaphors (autonomic); Intelligent microsystems.
Correction of current vulnerabilities	Tools and techniques to help system administrators fix current vulnerabilities; Human factors in security.
Denial-of-service attacks	Identify and deter denial-of-service and distributed denial-of-service attacks.
Detection, recovery, and survivability	Prediction of events; Reconstitution of system of systems; Autonomic computing; Global network surveillance and warning (similar to public health surveillance).
Law, policy, and economic issues	Market issues; Standards; Tradeoffs
Security engineering tools and techniques	Tools and methods for building more secure systems; Architecture for improved security; Formal methods; Programming languages that enforce security policy; Generative programming.
Security metrics	Data to support analysis; Metrics and models for economic analysis, risk analysis, etc.; Technical metrics to measure strength of security.
Security of foreign and mobile code	Ability to confine and encapsulate code; Tamper-proof software.
Security of network embedded systems	Security of real-time control systems such as SCADA.
Security policy management	Maintain a defined risk posture; Protect a defined security perimeter.
Traceback, forensics, and attribution of attacks	Correct attribution and retribution; Automatic counterattack.
Trust models for data and distributed applications	Peer-to-Peer (P2P) security; Establishing trust in data.
Vulnerability identification and analysis	Automated discovery and analysis of vulnerabilities; Code scanning tools; Device scanning.
Wireless security	Device and protocol level wireless security; Monitoring wireless network; Addressing DDoS attacks in wireless networks.

Source: GAO analysis.

Current research projects at universities and projects funded by several government agencies cover many of the research areas identified in the research agendas. Table 15 shows a sampling of some of the current research topics and is organized by the major control categories.

Table 15: Sampling of Current Research Topics

Control category	Research topics
Access controls	• Biometric access using facial recognition • Role-based access control
System integrity	• Storage devices that can detect changes to critical files • Network interfaces that can throttle worm/virus propagations • Software analysis for vulnerability detection • Code integrity verification • Proof-carrying code
Cryptography	• PKI for communications and computational security • Certification authority with defense against denial-of-service attacks • Quantum cryptography • Quantum key distribution
Audit and monitoring	• High-speed network monitoring for worm/virus detection • Emergent behavior detection • Honeynets to entice and deceive would-be attackers
Configuration management and assurance	• Survivable systems • Trusted computing • Evaluation and certification of systems

Source: GAO analysis.

Some researchers commented that the research topics are too often narrowly defined and focus on topics that are most likely to get funded. For example, research on automating security-related system administration tasks such as configuring or patching software does not get enough attention in the funded projects. The push to show results in a relatively short time causes researchers to avoid taking broad, system-wide views. Instead research projects look at narrowly scoped parts of a system. This tends to balkanize research projects and detract from a system-wide look at security.

Some researchers pointed out that academic research and corporate research seem to be on different paths. Corporate research tends to focus on improving existing product lines in the near-term, whereas university research typically looks at ideas irrespective of their viability as products. The transition from university research into products can be time-consuming and there is no well-defined approach.

Among some of the areas needing attention, researchers cited developing ways to measure security and assessing the economic effectiveness of proposed cybersecurity technologies. Such economic effectiveness studies can help make the case for specific cybersecurity technologies.

A long-term research objective is to develop systems that are inherently secure, with security engineered into the system from the start. Contrast this with current security technologies that are bolted on—added after the fact. A larger goal than security alone is to design and build survivable systems. Survivable systems have resiliency so that they can continue to perform, albeit at a degraded level, even when they are under attack. Such survivable systems require forethought in design, much as guardrails along dangerous curves are most effective only when they are built before anyone drives on the road. Survivability concepts can include the notion of defense-in-depth with defensive perimeters taken down to the level of system components such as storage devices and network interface cards and their associated software modules.

By comparing the identified research needs with the ongoing research, we arrive at the following research areas as a selection of some of the important areas that need continuing attention in cybersecurity research programs:

1. **Vulnerability identification and analysis**. There is a need for better methods to determine, throughout a product or system's life cycle (development, integration, update and maintenance, decommissioning, or replacement of components), whether exploitable defects have been introduced or unanticipated security problems have emerged. Research is needed into techniques and tools to analyze code, devices, and systems in dynamic and large-scale environments.

2. **Composing secure systems from insecure components**. Research is needed to develop approaches for composing complex heterogeneous systems that maintain security while recovering from failures. New approaches, such as the use of biological metaphors (autonomic) and intelligent microsystems, may be explored to create more secure systems.

3. **Security metrics and evaluation**. Research is needed to define metrics that express the costs, benefits, and impacts of security controls from multiple perspectives—economic, organizational, technical, and risk—so that the effect of security decisions can be better understood. Techniques are needed for modeling the security-

related behavior of systems and predicting the consequences of risk mitigation approaches.

4. **Wireless security**. In principle, many of the security concerns for wireless networks mirror those for the wired world; in practice, solutions that have been developed for wired networks may not be viable in wireless environments. Research is needed to make security a fundamental component of wireless networks, develop the basic science of wireless security, develop security solutions that can be integrated into the wireless device itself, investigate the security implications of existing wireless protocols, integrate security mechanisms across all protocol layers, and integrate wireless security into larger systems and networks. In particular, research is needed into security situational awareness techniques for wireless networks and strategies to address distributed denial-of-service attacks.

5. **Socioeconomic impact of security**. Research is needed to determine the scope and size of the cybersecurity problem and the effect that forces, such as laws, policy, and technology, have on infrastructure protection. For any technology, it is necessary to determine the legal, policy, and economic implications of the technology and its possible uses. Research is needed to describe the structure and dynamics of the cybersecurity marketplace. There is a need for research into the role of standards and best practices in improving cybersecurity posture, the policy and legal considerations relating to collection and use of data about the information infrastructures, and the implications of policies that are intended to direct responses to cyber attacks.

6. **Security for network embedded systems**. Research is needed on assessing the security of control systems that are prevalent in electricity, oil, gas, and water sectors. Security should be integrated into network embedded systems where previously it has not existed. Models of control networks can help in predicting the responses of control systems to changes and anomalies. Techniques are needed to detect, understand, and respond to anomalies in large, distributed control networks.

Some of these research areas are already receiving attention from the federal government. For example, NSF has recently announced a new program to foster cybersecurity research in areas such as trustworthy computing technology, evaluation and certification methods, efforts to prevent denial-of-service attacks, and long-term data-archiving technology. The NSF program also plans to support multidisciplinary research that covers the social, legal, ethical, and economic compromises that affect the

design and operation of secure network systems. The DHS Science and Technology Directorate is planning or has under way programs in the following areas: prevention and protection against attacks; monitoring, attack detection and response; mitigation of effects, remediation of damage, and recovery; and forensics and attribution. Other DHS research programs include infrastructure security (network protocols and process control systems) and foundations for cyber security (economic assessment activities, large scale data sets for testing).

Universities are also proposing research efforts to develop new science and technology for improving the cybersecurity of critical infrastructures. For example, recently teams of researchers from the University of California at Berkeley, Carnegie Mellon University, Cornell University, Stanford University, and Vanderbilt University have proposed a research center called the Team for Research in Ubiquitous Secure Technologies (TRUST) that would focus on designing systems that continue to work despite attacks or errors. The TRUST proposal presents three broad research categories—security technology, systems science, and social science. These categories are further broken down into 11 specific research areas that include topics such as software and network security, secure network embedded systems, and economics, public policy, and societal challenges of security.

As the federal government's research programs consider funding these cybersecurity research areas, it is important to note that there are many R&D needs vying for a limited amount of R&D dollars. Federal R&D program managers face tough choices in deciding where the R&D money should go and how much is appropriate for critical infrastructure protection. Depending on the infrastructure sector, it may be better to focus on overall infrastructure survivability, instead of the cybersecurity aspects alone. Some experts have suggested that if cybersecurity is deemed important to national security, it may be appropriate to adopt the R&D model adopted by DoD, where postulated threat models drive R&D in a progression from basic research through exploratory development, ending in government-funded engineering development of products and systems.

Addressing Long-Term Cybersecurity Research Needs

In addition to cybersecurity research that addresses existing cybersecurity threats, there is need for long-term research that anticipates the dramatic growth in the use of computing and networks. Some indicators of an upcoming period of dramatic growth include the increasing use of broadband networking technologies such as cable modems, the emergence of new wireless communication options, and the emergence of

Web Services that enable computers to communicate with one another directly using Web technologies.

High-speed networks and standards such as Web Services make it easy for an organization to connect its computers directly to the computers of its suppliers, but this surge in interconnections may bring a new wave of cybersecurity threats to a variety of critical business and government computing systems. Not enough is understood about security and reliability of these emerging complex systems. The rapid evolution of new styles of computing creates a pressing need for research into the fundamental options for securing Web Services and other complex, interconnected computing systems, and for ensuring that they will be reliable, highly available, self-managed, and self-repairing after disruption.

New options for connectivity and new wireless communication technologies also create new potential for undesired intrusion. Existing security research has focused more on establishing barriers against intrusion, with less attention to the preservation of personal privacy and the protection of intellectual property. New technical options are needed to protect privacy. Yet privacy is a two-edged sword because the same technologies that can protect private data may also help criminals and terrorists. Resolving such quandaries will require both technical advances as well as legal and social advances.

Recently, program managers at DARPA highlighted the Internet itself as perhaps the most serious security and reliability obstacle present in many sensitive military and intelligence systems. Increasing numbers of academic and commercial researchers echo these concerns. The Internet was created by a very cooperative, mutually trusting research community, and was designed with file transfers as its primary mission. This is simply not the appropriate model for applications such as broadband media transmission, highly available access to mission-critical services, or applications in which security and privacy are of primary importance. Although discarding the existing Internet does not make sense, researchers are suggesting an approach whereby the existing Internet hardware runs multiple side-by-side networks that might share the same hardware but have very different properties. However, like the development of the Internet itself, a substantial research investment would be required to achieve such new networks.

Table 16 lists some areas in which long-term research will be required. This research may occur in a diversity of settings, including academic institutions, government-funded small business innovation research

programs, and classified research programs that address the needs of military and intelligence communities.

Table 16: Sampling of Long-Term Research Areas

Research area	Description
Privacy	Better tools are needed for ensuring the privacy of sensitive information such as individual health records and financial records. Research is needed on the legal basis of privacy in an era of computer networks, on the emergence of new social patterns disruptive of traditional property ownership rules, and on technologies to enforce privacy.
Fault-tolerance	Some of the most disruptive cyber attacks start by provoking some form of failure or overload, causing the targeted system to degrade or become unresponsive. Technologies for embedding fault-tolerance into the major commercial platforms, such as Web services, are needed to greatly reduce the threat of such disruptions.
Scalability	As computing systems grow in size, enterprises are beginning to encounter problems of scale. Research is needed into managing systems that may include thousands or tens of thousands of machines. Progress in this area would reduce the cost of operating large systems.
New monitoring capabilities	Whereas computing systems of the past were relatively easy to instrument and monitor, the trend toward Web-based systems has created a new world in which an application may reside partly within a data center and partly on client systems spread over the Internet. New techniques are needed for monitoring such configurations, for diagnosing problems such as denial-of-service attacks and for reacting when problems occur.
Self-management	Existing computing systems often require human managers in rough proportion to the size of the system. Technology for self-management could enable deployment of large numbers of machines without a great deal of management and control by humans.
Self-healing	Technology is lacking for diagnosing the problem and carrying out an automated repair of systems that are damaged because of mundane problems or cyber attacks. Technology for building self-healing systems would be tremendously beneficial in a great variety of settings. This is a hard problem, because problems build on one another to produce a large number of symptoms that may vary greatly despite their common root cause.
Rearchitecting the Internet	It is time to revisit the core architecture of the Internet, moving from a “single network for all uses” model to one in which network connections might be portals to a small number of side-by-side networks, sharing the same hardware infrastructure but offering different properties. Development of such a capability will require many years of research but could ultimately provide better options for cybersecurity and robustness.

Source: Kenneth Birman, Cornell University.

Developing Approaches to Transition Research into Commercial Products

As we have described, there are many promising cybersecurity research projects ongoing in universities and government laboratories. For such research to be useful in improving the security of critical infrastructures, the results of the research must make their way into commercial products

and systems that can then be deployed in the infrastructures. This transition from research to actual products is not easy, and it takes time. The National Research Council has found that, for federal IT research, at least 10 years, and sometimes more than 15 years, elapse between initial research on a new idea and commercial success.[51] The council found that the relationship between government-funded research and industry research has been important in transitioning research results into commercial products.

Some have suggested the possibility of using a model based on SEMATECH—Semiconductor Manufacturing Technology—that was established by an act of Congress in 1987, when 14 U.S.-based semiconductor manufacturers and the U.S. government came together to strengthen the U.S. semiconductor industry. The consortium focused on solving common manufacturing problems by leveraging resources and sharing risks. By 1994, it had become clear that the U.S. semiconductor industry—both device makers and suppliers—had regained strength and market share; at that time, SEMATECH's board of directors voted to seek an end to matching federal funding after 1996, reasoning that the industry had returned to health and should no longer receive government support. Federal government may need to work with the computer security industry—the information technology sector—to develop options for migrating research results into IT products.

[51]National Research Council. *Innovation in Information Technology*, (Washington, D.C.: National Academy Press, 2003), 11.

Chapter 5: Summary

In this report we described a variety of cybersecurity technologies that can be used to help secure critical infrastructures from cyber attacks. Some technologies, such as firewalls and biometrics, can help to better protect computers and networks against attacks, while others, such as intrusion detection and continuity of operations tools, help to detect and respond to cyber attacks while they are in progress. These technologies can help to protect information that is being processed, stored, and transmitted in the networked computer systems that are prevalent in critical infrastructures. Although many cybersecurity technologies are available, experts feel that these technologies are not being purchased or implemented to their fullest extent. In addition to the need for a short-term solution of properly implementing current cybersecurity technologies, there is also a longer-term need for cybersecurity research and for transitioning the research results into commercially available products. On the basis of a number of research agendas and ongoing cybersecurity research, we found that a number of research areas need continuing attention. These cybersecurity research areas include composition of secure systems, security of network embedded systems, security metrics, socio-economic impact of security, vulnerability identification and analysis, and wireless security. Federal cybersecurity research programs are already beginning to address these research areas.

There are many implementation issues associated with using cybersecurity technologies for critical infrastructure protection. The issues include using a holistic approach to security, augmenting technology with people and processes, building security into new information systems, and considering non-technical options that can improve cybersecurity.

For a holistic approach to security, entities can use an overall security framework that includes a combination of risk assessments, security policies, security solutions, and security management, representing a continuous security process. Even when an entity has conducted a risk assessment and knows the extent of its cybersecurity needs, it cannot protect everything. Often, a business case is required to invest in cybersecurity. The interaction of technology with security processes and the people using the technology and the limitations of certain cybersecurity technologies can influence the purchase of technology. When building new information systems, organizations such as NIST have recommended that security requirements be considered as early as possible in the system development life cycle. System designers can use defense in depth—a strategy that uses a sequence of defensive mechanisms to enhance security.

Because critical infrastructures are so important to national security and the public good, the federal government has a stake in ensuring that the nation's critical infrastructures are protected. IT vendors provide the products, including cybersecurity technologies that entities use in their infrastructures. There are a number of opportunities for potential action by all stakeholders—from the entities to the government—in the areas of risk assessment, cybersecurity awareness, cybersecurity technology adoption and implementation, information sharing, cybersecurity research and development, and cybersecurity standards development. The federal government and other stakeholders already have several ongoing activities in these areas, which could help improve the cybersecurity posture in critical infrastructures.

Because the private sector owns most of the critical infrastructures, the federal government needs to gain insight into the infrastructures' vulnerabilities and relative priorities. The use of a risk-based framework for security and the conduct of risk assessments by infrastructure owners could provide the federal government with the information necessary to make informed policy decisions.

All federal actions have consequences—both intended and unintended. It would be irresponsible to propose or implement any action without examining the potential consequences, including the cost and benefits of the action. In particular, when discussing any potential action, it is crucial to carefully consider the following elements of a policy analysis framework:

- scope and size of the problem,
- market forces at play and their timeliness,
- level of organization of the critical infrastructure sectors and their ability to set and implement cybersecurity goals,
- costs and benefits of federal action,
- the intended and unintended consequences of federal action, and
- consequences of inaction by the federal government.

Although we focus primarily on federal actions, all levels of government—federal, state, and local—and the private sector have to work

cooperatively to improve the cybersecurity of our nation's critical computer-dependent infrastructures.

Critical infrastructure owners are ultimately responsible for the cybersecurity of the infrastructures. They can use a risk-based framework to select and implement available cybersecurity technologies. The federal government can consider a number of options to manage and encourage the increased use of cybersecurity technologies, support research and develop new cybersecurity technologies, and generally improve the level of cybersecurity of critical infrastructure sectors.

Agency Comments and Our Evaluation

We provided a draft of this report to the Department of Homeland Security and the National Science Foundation for their review.

We include DHS's comments in their entirety in appendix IV. We include NSF's comments in their entirety in appendix V.

Department of Homeland Security

In written comments on a draft of this report, the Department of Homeland Security stated that it generally concurred with the report. DHS said that the report effectively discusses many of the important cybersecurity issues and the report will be of great value to those entrusted with protecting critical systems and networks.

DHS provided technical comments on the draft, which we incorporated as appropriate. Specifically, DHS provided more details on its cybersecurity research and development programs and expressed concerns with our characterization of the breadth of cybersecurity research that is necessary. We agree that the cybersecurity research areas that we highlight in the report do not address all areas that require research funding. Our intent was to highlight some of the important research topics based on our review of cybersecurity research agendas and discussions with cybersecurity researchers. DHS suggested that we remove wireless security as a research area because funding is limited and there is a significant level of private sector activity and funding for wireless security. We consider wireless security an important area and wireless security appears in some well-known cybersecurity research agendas. Additionally, the list of research areas is meant to be for both government and private sector. We agree that federal R&D dollars are limited and not all research areas may be candidates for federal funding.

National Science Foundation

In written comments on a draft of this report, the National Science Foundation noted that this is an important and timely report that provides broad coverage of current and emerging cybersecurity and infrastructure technologies. NSF highlighted its engagement in the intertwined issues of critical infrastructure protection and computing. NSF went on to state that cybersecurity improvements may be made through the widespread deployment of architectures already recognized to be more resistant to attacks.

Citing new technology discoveries and major information technology shifts as drivers, NSF emphasized the critical ongoing role of long range research both for developing newly robust infrastructures and for achieving security as an inherent property of these infrastructures. Finally, NSF noted that an essential component of security is the use of credible deterrents. NSF believes that research in cyber forensics and its effective use by law enforcement may reduce the overall threat and serve as a deterrent to would-be attackers.

External Review Comments

We provided a draft of this report to 26 organizations, including representatives of six critical infrastructure sectors, for their review. Individuals from these organizations were selected because of their assistance during the data collection phase of our work or their attendance at our cybersecurity meeting, convened for us by the National Academy of Sciences. The reviewers represented government, industry, and academia. We received comments and suggestions from 15 reviewers. The comments ranged from clarifying issues to highlighting certain aspects of the assessment that the reviewers considered important. We have incorporated these comments, where appropriate, in the report.

Several reviewers commended us for putting together a good report. One reviewer congratulated us for pulling such challenging material into an exceptionally coherent and solid document. Another reviewer felt that the report is very thorough and manages to stay on task given the scope and complexity of the issues.

Among the detailed comments, one suggestion was to briefly discuss long-term research that takes into account an anticipated dramatic growth in the use of computing and networks. We added a section on long-term research that includes a table with a sampling of research areas. A reviewer noted that run-of-the-mill poor systems management can be as serious a threat as a deliberate cyber attack. The reviewer characterized such poor systems management as a mundane cybersecurity threat. On the

basis of that reviewer's suggestion we included a discussion of the serious consequences of such routine mismanagement.

Another reviewer stated that the report is no longer relevant because waves of worm/virus attacks in recent months have made the Internet a far more dangerous place and that any risk management approach would be problematic. We disagree with this characterization and believe that the threats to both the Internet and other critical infrastructure networks continue to be relevant and that risk management remains a logical approach to addressing the cybersecurity needs of critical infrastructures.

Comments from the critical infrastructure sectors were generally favorable. One sector representative commented that the report strikes a reasonably good balance between analysis and recommendations, and that the three key questions that provide the overall structure for the report are relevant and timely. Some sector representatives also provided clarifying details about information related to their sector. For example, one sector representative cited a recent government grant to help support that sector's ISAC. Another sector representative clarified how a segment of that sector relies on information technology for its operations. We incorporated the sector-suggested clarifications and changes as appropriate.

Appendix I: Technology Assessment Methodology

This technology assessment focuses on three key questions:

1. What are the key cybersecurity requirements in each of the critical infrastructure protection sectors?

2. What cybersecurity technologies can be applied to critical infrastructure protection? What technologies are currently deployed or currently available but not yet widely deployed for critical infrastructure protection? What technologies are currently being researched for cybersecurity? Are there any gaps in cybersecurity technology that should be better researched and developed to address critical infrastructure protection?

3. What are the implementation issues associated with using cybersecurity technologies for critical infrastructure protection, including policy issues such as privacy and information sharing?

To identify cybersecurity technologies that can be used for critical infrastructure protection (CIP), we reviewed relevant cybersecurity reports and vendor literature. We met with representatives of the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), the Infosec Research Council, and the Department of Homeland Security's (DHS) Science and Technology directorate to discuss current and planned federal cybersecurity research efforts. We also met with representatives from two Department of Energy national labs, Sandia National Labs and Lawrence Livermore National Lab, and one Department of Defense center, the CERT Coordination Center (CERT/CC).[1] We interviewed cybersecurity researchers from academic institutions (Carnegie Mellon University, Dartmouth College, and the University of California at Berkeley) and corporate research centers (AT&T Research Labs, SRI International, and HP Labs).

To identify the key cybersecurity requirements in each critical infrastructure sector, we developed a data collection instrument and used it to interview sector representatives such as industry groups or companies within the sector. We used the critical infrastructure sectors

[1]The CERT/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

defined in the Administration's national strategy documents.[2] We interviewed representatives from the Banking and Finance, Chemical Industry and Hazardous Materials, Defense Industrial Base, Energy, Information and Telecommunications, Transportation, and Water sectors. We met with officials from DHS's Information Analysis and Infrastructure Protection (IAIP) directorate to discuss their efforts in organizing and coordinating CIP activities. We also met with IAIP's National Communications System (NCS), which operates the information-sharing and analysis center (ISAC) for the telecommunications sector. We met with the Coast Guard to discuss its efforts in the maritime transportation sector.

To identify implementation issues, we reviewed previous studies on security and CIP, including those from the National Research Council, CERT/CC, the Institute for Information Infrastructure Protection (I3P), and NIST. We interviewed critical infrastructure sector representatives to identify the challenges they face in implementing cybersecurity technologies. We also relied on previous GAO reports on cybersecurity and CIP. To examine policy issues, we reviewed current federal statutes and regulations that govern the protection of computer systems. On the basis of information that we collected through literature reviews and interviews, we assessed the effects of several policy options that could be employed by the federal government.

In October 2003, we convened a meeting, with the assistance of the National Academy of Sciences (NAS), to review the preliminary results of our work.[3] Meeting attendees included representatives from academia, critical infrastructure sectors, and public policy organizations.

We provided a draft of this report to DHS and NSF for their review. We include their comments in appendixes IV and V, respectively. In addition, we provided a draft of this report to selected attendees of the meeting that

[2]The White House, Office of Homeland Security, *National Strategy for Homeland Security*, (Washington, D.C.: July 2002) and The White House, *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*, (Washington, D.C.: Feb. 2003).

[3]We have a standing contract with NAS under which NAS provides assistance in convening groups of experts to provide information and expertise to our engagements. NAS uses its scientific network to identify participants and uses its facilities and processes to arrange the meetings. Recording and using the information in a report is our responsibility.

we convened with NAS for this work and with other interested organizations.

We conducted our work from May 2003 to February 2004 in the Washington, D.C., metropolitan area; the San Francisco, California, metropolitan area; Princeton, New Jersey; and Pittsburgh, Pennsylvania. We performed our work in accordance with generally accepted government auditing standards.

Appendix II: Summary of Federal Critical Infrastructure Protection Policies

Over the years, several working groups have been formed, special reports written, federal policies issued, and organizations created to address CIP. Although these steps have raised awareness and spurred activity by many critical infrastructures and the federal government, the nation still faces several challenges in CIP. To provide a historical perspective, table 17 summarizes the key developments in federal CIP policy since 1997. Four key actions that have shaped the development of the federal government's CIP policy are

- Presidential Decision Directive 63 (PDD 63)
- Homeland Security Act of 2002
- The National Strategy to Secure Cyberspace
- Homeland Security Presidential Directive 7 (HSPD-7)

Table 17: Federal Government Actions Taken to Develop CIP Policy

Policy action	Date	Description
Critical Foundations: Protecting America's Infrastructures[a]	Oct. 1997	Described the potentially devastating effects of poor information security for the nation and recommended measures to achieve a higher level of CIP that included industry cooperation and information sharing, a national organizational structure, a revised program of research and development, a broad program of awareness and education, and a reconsideration of related laws.
Presidential Decision Directive 63	May 1998	Established CIP as a national goal and presented a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. Established government agencies to coordinate and support CIP efforts. Identified lead federal agencies to work with coordinators in eight infrastructure sectors and five special functions. Encouraged the development of information-sharing and analysis centers.
National Plan for Information Systems Protection[b]	Jan. 2000	Provided a vision and framework for the federal government to prevent, detect, and respond to attacks on the nation's critical cyber-based infrastructure and to reduce existing vulnerabilities by complementing and focusing existing federal computer security and information technology requirements.
Executive Order 13228	Oct. 2001	Established the Office of Homeland Security within the Executive Office of the President to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. Established the Homeland Security Council to advise and assist the President with all aspects of homeland security and to ensure coordination among executive departments and agencies.

Policy action	Date	Description
Executive Order 13231	Oct. 2001	Established the President's Critical Infrastructure Protection Board to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures and to recommend policies and coordinating programs for protecting CIP-related information systems.
National Strategy for Homeland Security[c]	July 2002	Identified the protection of critical infrastructures and key assets as a critical mission area for homeland security. Expanded the number of critical infrastructures to 13 from the 8 identified in PDD 63 and identified lead federal agencies for each.
Homeland Security Act of 2002[d]	Nov. 2002	Created the Department of Homeland Security and assigned it the following CIP responsibilities: (1) developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States; (2) recommending measures to protect the key resources and critical infrastructures of the United States in coordination with other groups; and (3) disseminating, as appropriate, information to assist in the deterrence, prevention, preemption of, or response to terrorist attacks.
The National Strategy to Secure Cyberspace[e]	Feb. 2003	Provided the initial framework for both organizing and prioritizing efforts to protect our nation's cyberspace. Provided direction to federal departments and agencies that have roles in cyberspace security and identified steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity.
The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets[f]	Feb. 2003	Provided a statement of national policy to remain committed to protecting critical infrastructures and key assets from physical attacks. Built on PDD 63 with its sector-based approach and called for expanding the capabilities of ISACs. Outlined three key objectives: (1) identifying and assuring the protection of the most critical assets, systems, and functions; (2) assuring the protection of infrastructures that face an imminent threat; and (3) pursuing collaborative measures and initiatives to assure the protection of other potential targets.
Executive Order 13286	Feb. 2003	Superseded Executive Order 13231 but maintained the same national policy statement regarding the protection against disruption of information systems for critical infrastructures. Dissolved the President's Critical Infrastructure Protection Board and eliminated the board's chair, the Special Advisor to the President for Cyberspace Security. Designated the National Infrastructure Advisory Council to continue to provide the President with advice on the security of information systems for critical infrastructures supporting other sectors of the economy through the Secretary of Homeland Security.

Policy action	Date	Description
Homeland Security Presidential Directive 7	Dec. 2003	Superseded PDD 63 and established a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attack. Defined roles and responsibilities for the Department of Homeland Security and sector-specific agencies to work with sectors to coordinate CIP activities. Established a CIP Policy Coordinating Committee to advise the Homeland Security Council on interagency CIP issues.

Source: GAO analysis.

[a]President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C.: Oct. 1997).

[b]The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to Dialogue* (Washington, D.C.: Jan. 2000).

[c]The White House, Office of Homeland Security, *National Strategy for Homeland Security*.

[d]Homeland Security Act of 2002, Public Law 107-296 (Nov. 25, 2002).

[e]The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: Feb. 2003).

[f]The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.

Presidential Decision Directive 63 Established Initial CIP Strategy

In 1998, the President issued PDD 63, which described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. PDD 63 called for a range of actions that were intended to improve federal agency security programs, improve the nation's ability to detect and respond to serious computer-based and physical attacks, and establish a partnership between the government and the private sector. The directive called on the federal government to serve as a model of how infrastructure assurance is best achieved, and it designated lead agencies to work with private sector and government entities. Further, it established CIP as a national goal and stated that, by the close of 2000, the United States was to have achieved an initial operating capability to protect the nation's critical infrastructures from intentional destructive acts and, by 2003, have developed the ability to protect the nation's critical infrastructures from intentional destructive attacks.

To accomplish its goals, PDD 63 established and designated organizations to provide central coordination and support, including

- the Critical Infrastructure Assurance Office (CIAO), an interagency office housed in the Department of Commerce, which was established to develop a national plan for CIP based on infrastructure plans that had been developed by the private sector and federal agencies;

- the National Infrastructure Protection Center (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response; and

- the National Infrastructure Assurance Council, which was established to enhance the partnership of the public and private sectors in protecting our critical infrastructures.[1]

To ensure the coverage of critical sectors, PDD 63 identified eight infrastructures: (1) banking and finance; (2) information and communications; (3) water supply; (4) aviation, highway, mass transit, pipelines, rail, and waterborne commerce; (5) emergency law enforcement; (6) emergency fire services and continuity of government; (7) electric power and oil and gas production and storage; and (8) public health services. It also identified five special functions: (1) law enforcement and internal security, (2) intelligence, (3) foreign affairs, (4) national defense, and (5) research and development. For each of the infrastructures and functions, the directive designated lead federal agencies, referred to as sector liaisons, to work with their counterparts in the private sector, referred to as sector coordinators. To facilitate private sector participation, PDD 63 also encouraged the voluntary creation of ISACs to serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC.

PDD 63 called for a range of activities that were intended to establish a partnership between the public and private sectors to ensure the security of our nation's critical infrastructures. Sector liaisons and sector coordinators were to work together to address problems related to CIP for each sector. In particular, PDD 63 stated that they were to (1) develop and implement vulnerability awareness and education programs, and (2) contribute to a sector National Infrastructure Assurance Plan by

[1]Executive Order 13231 replaced this council with the National Infrastructure Advisory Council.

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing major attacks; and
- developing a plan for alerting, containing, and rebuffing an attack in progress and then, in coordination with the Federal Emergency Management Agency, as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

PDD 63 also required every federal department and agency to be responsible for protecting its own critical infrastructures, including both cyber-based and physical assets. To fulfill this responsibility, PDD 63 called for agencies' chief information officers to be responsible for information assurance, and it required every agency to appoint a chief infrastructure assurance officer to be responsible for the protection of all other aspects of an agency's critical infrastructure. Further, it required federal agencies to

- develop, implement, and periodically update a plan for protecting its critical infrastructure;
- determine its minimum essential infrastructure that might be a target of attack;
- conduct and periodically update vulnerability assessments of its minimum essential infrastructure;
- develop a recommended remedial plan, based on vulnerability assessments, that identifies time lines for implementation, responsibilities, and funding; and
- analyze intergovernmental dependencies and mitigate those dependencies.

Other PDD 63 requirements for federal agencies included providing vulnerability awareness and education to sensitize people regarding the importance of security and training them in security standards, particularly regarding computer systems; establishing a system for responding to significant ongoing infrastructure attacks to help isolate and minimize damage; and establishing a system for rapidly reconstituting minimum required capabilities for varying levels of successful infrastructure attacks.

The Homeland Security Act of 2002 Created the Department of Homeland Security

The Homeland Security Act of 2002, signed by the President on November 25, 2002, established the Department of Homeland Security. The act assigned the department a number of CIP responsibilities, including: (1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States; (2) recommending measures to protect the key resources and critical infrastructure of the United States in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities; and (3) disseminating, as appropriate, information analyzed by the department both within the department and to other federal agencies, state and local government agencies, and private sector entities to assist in the deterrence, prevention, preemption of, or response to terrorist attacks.

To help accomplish these functions, the act created the Information Analysis and Infrastructure Protection Directorate within the department and transferred to it the functions, personnel, assets, and liabilities of several existing organizations with CIP responsibilities, including NIPC (not including the Computer Investigations and Operations Section) and CIAO.

The National Strategy to Secure Cyberspace Provided an Initial Cyber CIP Framework

The National Strategy to Secure Cyberspace is intended to provide an initial framework for both organizing and prioritizing efforts to protect our nation's cyberspace. It also provided direction to federal departments and agencies that have roles in cyberspace security and identified steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. The strategy lists the critical infrastructure sectors and the related lead federal agencies that are identified in the *National Strategy for Homeland Security*, which expanded the number of critical infrastructures from the 8 defined in PDD 63 to 13. In addition, the strategy identifies DHS as the central coordinator for cyberspace efforts. As such, DHS is responsible for coordinating and working with other federal entities that are involved in cybersecurity.

The National Strategy to Secure Cyberspace is organized according to five national priorities, with major actions and initiatives identified for each.

1. Security Response System—provides a public/private architecture for analyzing, warning, and managing incidents of national significance, promoting continuity in government systems and private sector infrastructures, and increasing information sharing.

2. Threat and Vulnerability Reduction Program—reduces threats and deters malicious actions through effective programs to identify and punish violators, identifies and remediates existing vulnerabilities, develops new systems with fewer vulnerabilities, and assesses emerging technologies for vulnerabilities.

3. Awareness Training—emphasizes the promotion of a comprehensive national awareness program to empower all Americans to secure their own parts of cyberspace.

4. Securing Government's Cyberspace—protects, improves, and maintains the federal government's cybersecurity.

5. National Security and International Cyberspace Security Cooperation—identifies major actions and initiatives to strengthen the U.S. national security and international cooperation.

Homeland Security Presidential Directive 7 Defined Federal CIP Responsibilities

In December 2003, the President issued HSPD-7, which established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources and to protect them from terrorist attack and superseded PDD-63. HSPD-7 defines responsibilities for DHS, lead federal agencies, or sector-specific agencies, that are responsible for addressing specific critical infrastructure sectors, and other departments and agencies. It instructs federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks. To accomplish these tasks, the federal government is to work with state and local governments and the private sector.

The Secretary of Homeland Security is assigned several responsibilities, including:

- coordinating the national effort to enhance critical infrastructure protection;
- identifying, prioritizing, and coordinating the protection of critical infrastructure, emphasizing protection against catastrophic health effects or mass casualties;
- establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors; and

- serving as the focal point for security of cyberspace, including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for critical infrastructure information systems.

To ensure the coverage of critical sectors, HSPD-7 designated sector-specific agencies for the critical infrastructure sectors identified in the *National Strategy for Homeland Security* (see table 18). These agencies are responsible for infrastructure protection activities in their assigned sectors and are to coordinate and collaborate with relevant federal agencies, state and local governments, and the private sector to accomplish these responsibilities. Specifically, sector-specific agencies are to conduct or facilitate vulnerability assessments of the sector and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructures. In addition, they are to identify, prioritize, and coordinate the protection of critical infrastructures and facilitate the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. Sector-specific agencies are to report to DHS on an annual basis on their activities to meet these responsibilities. Further, the sector-specific agencies are to continue to encourage the development of information-sharing and analysis mechanisms and to support sector-coordinating mechanisms.

Table 18: Critical Infrastructure Sectors Identified by the National Strategy for Homeland Security and HSPD-7

Sector	Description	Sector-specific agencies
Agriculture	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production.	Department of Agriculture
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions including clearing and settlement.	Department of the Treasury
Chemicals and hazardous materials	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical industry represents a $450 billion enterprise and produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction and other necessities.	Department of Homeland Security
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	Department of Homeland Security
Energy	Provides the electric power used by all sectors, including critical infrastructures, and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Food	Carries out the post-harvesting of the food supply, including processing and retail sales.	Department of Agriculture and Department of Health and Human Services
Government	Ensures national security and freedom and administers key public functions.	Department of Homeland Security
Information technology and telecommunications	Provides communications and processes to meet the needs of businesses and government.	Department of Homeland Security
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector.	Department of Homeland Security
Public health and healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Transportation	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	Department of Homeland Security
Drinking water and water treatment systems	Sanitizes the water supply with the use of about 170,000 public water systems. These systems depend on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.	Environmental Protection Agency

Source: GAO analysis based on the President's National Strategy documents and HSPD-7.

By December 2004, the Secretary of Homeland Security also is to produce a comprehensive and integrated national plan for critical infrastructure and key resources protection that will outline national goals, objectives, milestones, and key initiatives. If appropriate, the plan is also to include:

- a strategy to identify, prioritize, and coordinate the protection of critical infrastructures, including an approach for how DHS will coordinate with other federal agencies, state and local governments, the private sector, foreign countries, and international organizations;
- a summary of activities to define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructures;
- a summary of initiatives for sharing critical infrastructure information and for providing threat warning data to state and local governments and the private sector; and
- coordination and integration with other federal emergency management and preparedness activities, such as the National Response Plan.

To support information-sharing efforts, HSPD-7 instructs the Secretary of Homeland Security to establish appropriate systems, mechanisms, and procedures to share homeland security information on threats and vulnerabilities in critical infrastructures with other federal agencies, state and local governments, and the private sector in a timely manner.

HSPD-7 establishes a CIP Policy Coordinating Committee, which will advise the Homeland Security Council on interagency policy related to physical and cyber infrastructure protection. The Office of Science and Technology Policy (OSTP) will coordinate interagency research and development to enhance CIP activities. In coordination with OSTP, DHS is to prepare an annual federal research and development plan to support critical infrastructure protection activities. To better understand the potential effects of attacks on the critical infrastructure, DHS is to develop models on the potential implications of attacks on critical infrastructures, focusing on densely populated areas. Further, DHS is to develop a national indications and warnings architecture for infrastructure protection that will facilitate (1) an understanding of baseline infrastructure operations; (2) the identification of indicators and precursors to an attack; and (3) surge capacity for detecting and analyzing potential attack patterns.

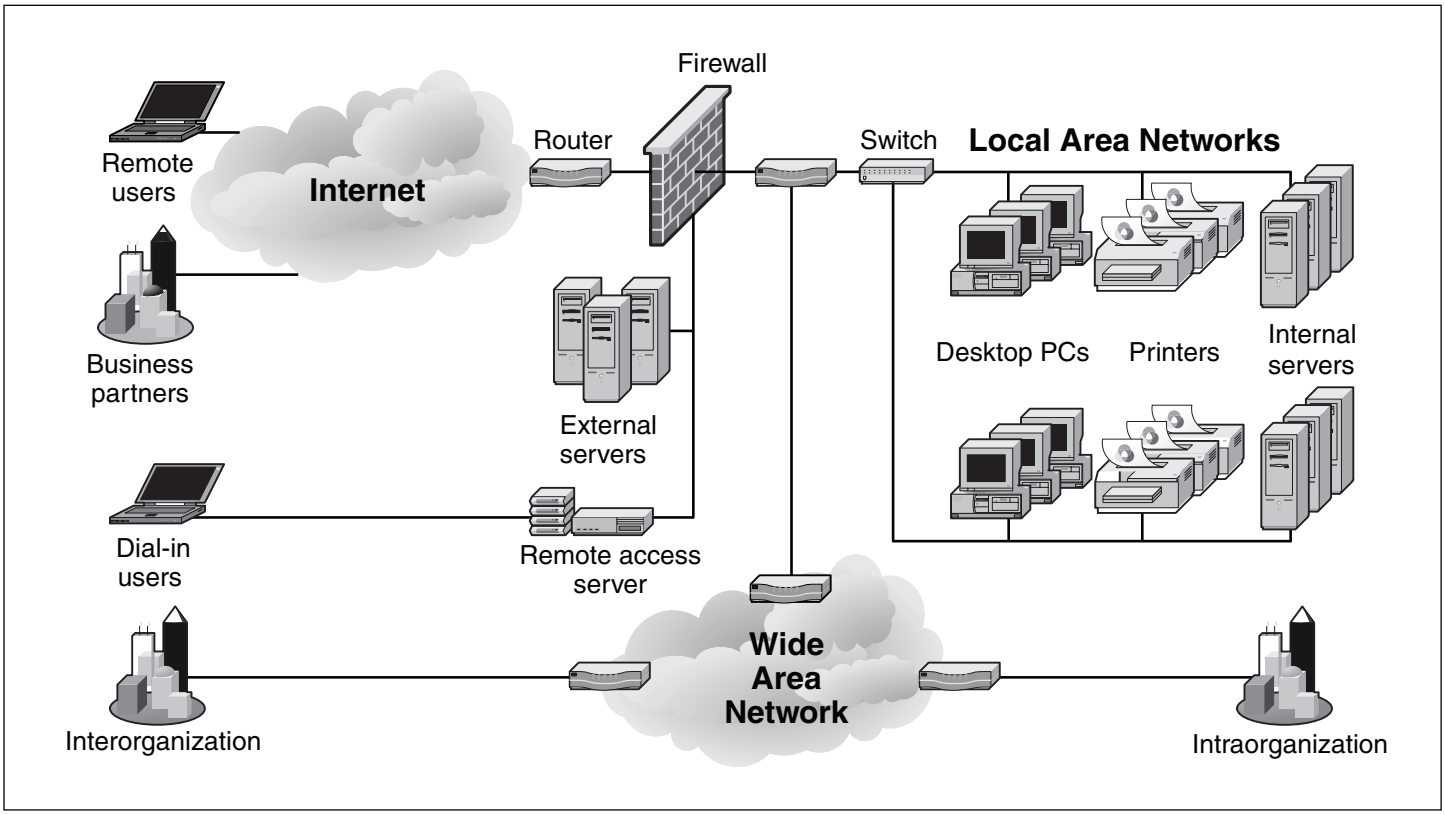
Consistent with PDD 63, HSPD-7 requires all federal departments and agencies to be responsible for protecting their own internal critical infrastructure. These agencies are to develop plans for the protection of their physical and cyber critical infrastructures and to provide them to the Office of Management and Budget for approval by July 2004. These plans are to address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.

Appendix III: Cybersecurity Technologies

Overview of Network Systems

Computer systems are most visible in the information technology (IT) that organizations use in their data, voice, and video centers and that workers use on their desks and for remote access. Computers, in many different forms, are also embedded in many systems that run infrastructures in sectors ranging from electric power systems to medical, police, fire, and rescue systems. Infrastructures use interconnected computer systems extensively. These networks of computer systems consist of host computers that are connected by communication links, which can be wired or wireless. We use the term *host* to refer to a computer of any form—a mainframe, a server, or a desktop personal computer (PC), as well as other, less obvious computers, such as a router or a real-time process-control computer. Hosts store information and run software, typically an operating system and one or more application programs. The term *network* refers to the data communication links and the network elements such as routers, hubs, and switches that enable the hosts to communicate with each other. The network systems infrastructure can be viewed as an interconnected collection of hosts and networks, as illustrated in figure 8.

Figure 8: An Example of Typical Networked Systems



Source: GAO analysis and Microsoft Visio.

As figure 8 shows, computer systems are interconnected by networks, which, in turn, are often connected to the Internet—the worldwide collection of networks, operated by some 10,000 Internet Service Providers (ISP). Most organizations have one or more local area networks (LANs) at each of their offices. Larger organizations also have wide area networks (WANs) that connect the organization's various offices in different geographical locations.

There Are Different Types of Hosts

The hosts in these network systems can be grouped into four main types according to their typical usage:

- **Mainframes** are large computers that are capable of supporting thousands of simultaneous users. Although historically they have been associated with centralized computing, today's mainframes can be used

in networks to serve distributed users and smaller servers. Hitachi and IBM are examples of mainframe computer manufacturers.

- **Mid-range systems** are powerful computers that often are used in corporate settings as servers or single-user computers. Mid-range system manufacturers include Hewlett-Packard, IBM, and Sun Microsystems.
- **Personal computers** are small, relatively inexpensive computers that are designed for a single user. Although they vary in speed and performance, PCs use microprocessors and have self-contained data storage devices. PC manufacturers include Apple, Dell, Gateway, Hewlett-Packard, and IBM.
- **Embedded systems** are specialized computer systems that are part of a larger system or machine. Typically, an embedded system is housed on a single microprocessor board with the programs stored in read-only memory. Virtually all appliances that have a digital interface—for example, watches, microwaves, video cassette recorders (VCR), digital video disk (DVD) players, and cars—utilize embedded systems.

Whether it is a large mainframe computer or a desktop PC, each host has three basic components: (1) a central processing unit (CPU), which performs the instructions that are contained in a computer program; (2) random access memory (RAM), which stores computer programs and information while the CPU is processing them; and (3) permanent storage media, such as hard disk, read-only memory (ROM), or CD-ROM, which serves as the permanent storage space for computer programs and data. In addition to these basic components—CPU, memory, and permanent storage—a host typically has other devices attached to it. These devices can range from the network interface that connects the computer to the network to user input/output devices such as keyboards, monitors, and printers.

Hosts Run Operating Systems and Applications

Each host computer typically runs an *operating system*. The operating system is a special collection of computer programs that has two primary purposes. First, operating systems provide the interface between application programs and the CPU and other hardware components. Second, operating systems load and run other programs. All operating systems include one or more command processors that allow users to type commands and perform tasks like running a program or printing a file. Most operating systems also include a graphical user interface that enables the user to perform most tasks by clicking on-screen icons. Some examples of operating systems are Microsoft Windows, Unix, Linux, OS/390, z/OS, and Mac OS.

Some embedded systems include an operating system, but many are so specialized that the entire logic can be implemented as a single program. Embedded systems are widely used in many critical infrastructures.

Computer application programs make use of the capabilities that the operating system provides. For example, computer programs read and write files by using built-in capabilities of the operating system.

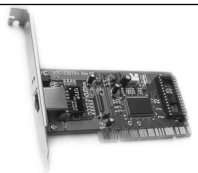
Operating systems include some built-in security features like user names, passwords, and permissions, to perform specific tasks, such as running certain applications or accessing specific information such as a file or a database.

Networks Use Protocols

Networks use a predefined set of rules known as protocols to communicate with each other. For example, the Transmission Control Protocol/Internet Protocol (TCP/IP) suite is the protocol of choice on the Internet. A *network protocol* refers to a detailed process the sender and receiver agree upon for exchanging data.

TCP/IP networking can best be explained and understood in terms of a model with four layers, where each layer is responsible for performing a particular task. The layered model describes the flow of data between the physical connection to the network and the end-user application. Figure 9 shows the four-layer network model for TCP/IP.

Figure 9: TCP/IP Four-layer Network Model

Application	**SMTP** (Simple Mail Transfer Protocol), **FTP** (File Transfer Protocol), **HTTP** (Hyper Text Transfer Protocol) (Web), **Telnet**, **DNS** (Domain Name System), and **RTP/RTCP** (Real-Time Transport Protocol/Real-Time Control Protocol) (audio and video streams)
Transport	**TCP** (Transmission Control Protocol), **UDP** (User Datagram Protocol)
Network	**IP** (Internet Protocol)
Physical	

Source: GAO.

In this four-layer model, information always moves from one layer to the next. For example, when an application sends data to another application, the data go through the layers in this order: Application—>Transport —>Network—>Physical. At the receiving end, the data go up from Physical—>Network—>Transport—>Application.

Each layer has its own set of protocols for handling and formatting the data. The way in which data are sent on a network is similar to the way in which letters are sent through the postal service. For example, a typical protocol involved in sending a letter would be a preferred sequence of data for a task such as addressing an envelope (first the name; then the street address; and then city, state, and zip or other postal code). Similarly, a protocol in the network layer of TCP/IP might be to prepare a packet for transmission from one network to another. There would be some information in that packet identifying the network where the packet originated as well as the destination network. Software that implements the TCP/IP protocols is typically included as part of the operating system.

Each of the four layers performs a specialized function:

- **Application layer**: Applications such as e-mail readers and Web browsers interface with the application layer to transmit data over TCP/IP networks. There are application-level protocols such as Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) for e-mail; Hyper Text Transfer Protocol (HTTP) for the Web; File Transfer Protocol (FTP) for file transfers; and Real-Time Transport Protocol/Real-Time Control Protocol (RTP/RTCP) for delivery of audio and video streams. Application-level protocols also have a port number that can be thought of as an identifier for a specific application. For example, port 80 is associated with HTTP or a Web server.

- **Transport layer**: This layer breaks large messages into data packets for transmission and reassembles them at the destination. The two most important protocols in this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP guarantees delivery of data; UDP just sends the data without ensuring that it actually reaches its destination.

- **Network layer**: This layer is responsible for getting data packets from one network to another. If the networks are far apart, the data packets are routed from one network to the next until they reach their destination. The primary protocol in this layer is the Internet Protocol (IP).

- **Physical layer**: This layer consists of the physical networking hardware (such as an Ethernet card or Token Ring card) that carries the data packets in a network.

The benefit of the layered model is that each layer takes care of only its specific task, leaving the rest to the other layers. The layers can mix and match—TCP/IP networks can work over any type of physical network medium, from Ethernet to radio waves (in a wireless network). In addition, each layer can be implemented in different modules. For example, typically the transport and network layers already exist as part of the operating system, and any application can make use of these layers.

TCP/IP Networks Use IP Addresses to Identify Networks and Hosts

TCP/IP networks such as the Internet comprise many networks as well as many hosts on each network. Each host in a TCP/IP network is identified by its IP address. Because TCP/IP deals with internetworking—interconnecting many networks—the IP address is a network address that

identifies the network on which the host is located and a host address that identifies the specific computer on that network. The IP address is a 4-byte (32-bit) value. The convention is to write each byte as a decimal value and to put a dot (.) after each number. For example, a typical IP address might be 192.168.0.1. This way of writing IP addresses is known as dotted-decimal or dotted-quad notation. In decimal notation, a byte (which is made up of 8 bits) can have a value between 0 and 255. Thus a valid IP addresses can use only the numbers between 0 and 255 in the dotted-decimal notation. The numbers 0 and 255 in the network or host address part of the IP address have special meanings.

Internet Services Use Well-Known Port Numbers

The TCP/IP protocol suite has become the de facto communications standard of the Internet because many standard services are available on all systems that support TCP/IP. These services make the Internet useful by enabling the transfer of mail, news, and Web pages. A well-known port is associated with each of these services. A transport layer protocol, such as TCP, uses this port to locate a service on any system. A server process—a computer program running on a system—implements each service. These services include

- **DHCP (Dynamic Host Configuration Protocol)** is used to dynamically configure TCP/IP network parameters on a computer. DHCP is primarily used to assign dynamic IP addresses and other networking information such as name server, default gateway, and domain names that are needed to configure TCP/IP networks. The DHCP server listens on port 67.
- **FTP (File Transfer Protocol)** enables the transfer of files between computers over the Internet. FTP uses two ports—data is transferred on port 20, while control information is exchanged on port 21.
- **HTTP (Hypertext Transfer Protocol)** is a recent protocol for sending Hypertext Markup Language (HTML) documents from one system to another. HTTP is the underlying protocol of the Web. By default, the Web server and client communicate on port 80.
- **NFS (Network File System)** is for sharing files among computers. NFS uses Sun's Remote Procedure Call (RPC) facility, which exchanges information through port 111.
- **NNTP (Network News Transfer Protocol)** is for distribution of news articles in a store-and-forward fashion across the Internet. NNTP uses port 119.
- **SMTP (Simple Mail Transfer Protocol)** is for exchanging e-mail messages between systems. SMTP uses port 25 for information exchange.

- **Telnet** enables a user on one system to log into a remote system on the Internet (the user must provide a valid user ID and password to log into the remote system). Telnet uses port 23 by default.
- **SNMP (Simple Network Management Protocol)** is used to manage all types of network devices on the Internet. Like FTP, SNMP uses two ports: 161 and 162.

Current Cybersecurity Technologies

There are several technologies that can be used by critical infrastructure owners to enhance their cybersecurity postures.[1] While several classifications of cybersecurity technologies are available, we present a taxonomy based on controls. Security controls are the management, operational, and technical safeguards that are used to protect a system and its information. Table 19 lists the five control categories and control types that support these categories. Several different technologies are available that provide functionality in support of these control categories and types. Some technologies can support more than one control type. Some of these technologies are implemented on hosts and network elements as "add-on" functionality. Other cybersecurity technologies are sold as integrated hardware and software platforms.

[1]GAO has previously reported on cybersecurity technologies available to help secure federal computer systems. See U.S. General Accounting Office, *Information Security: Technologies to Secure Federal Systems*, GAO-04-467 (Washington, D.C.: March 9, 2004).

Table 19: Cybersecurity Technology Control Categories and Types

Control category	Control type
Access controls	
• Boundary protection	• Firewalls • Content management
• Authentication	• Biometrics • Smart tokens
• Authorization	• User rights and privileges
System integrity	• Antivirus software • File integrity checkers
Cryptography	• Digital signatures and certificates • Virtual private networks
Audit and monitoring	• Intrusion detection systems • Intrusion prevention systems • Security event correlation tools • Computer forensics tools
Configuration management and assurance	• Policy enforcement applications • Network management • Continuity of operations • Scanners • Patch management

Source: GAO analysis.

Access Controls

Access control technologies ensure that only authorized users or systems can access and use computers, networks, and the information stored on these systems and help to protect sensitive data and systems. Access control simplifies network security by reducing the number of paths that attackers might use to penetrate system or network defenses. Access control includes three different control types: boundary protection, authentication, and authorization.

Boundary protection technologies demark a logical or physical boundary between protected information and systems and unknown users. Boundary protection technologies can be used to protect a network (for example, firewalls) or a single computer (for example, personal firewalls). Generally, these technologies prevent access to the network or computer by external unauthorized users. Another type of boundary protection technology, content management, can also be used to restrict the ability of

authorized system or network users to access systems or networks beyond the system or network boundary.

Authentication technologies associate a user with a particular identity. People are authenticated by three basic means: by something they know, something they have, or something they are. People and systems regularly use these means to identify people in everyday life. For example, members of a community routinely recognize one another by how they look or how their voices sound—by something they are. Automated teller machines recognize customers because they present a bank card—something they have—and they enter a personal identification number (PIN)—something they know. Using a key to enter a locked building is another example of using something you have. More secure systems may combine two of more of these approaches.

While the use of passwords is an example of authentication based on something users know, there are several technologies based on something users have. Security tokens can be used to authenticate a user. User information can be coded onto a token using magnetic media (for example, bank cards) or optical media (for example, compact disk-like media). Several smart token technologies containing an integrated circuit chip that can store and process data are also available. Biometric technologies automate the identification of people using one or more of their distinct physical or behavioral characteristics—authentication based on something that users are. The use of security tokens or biometrics requires the installation of the appropriate readers at network and computer access points.

Once a user is authenticated, authorization technologies are used to allow or prevent actions by that user according to predefined rules. Users could be granted access to data on the system or to perform certain actions on the system. Authorization technologies support the principles of legitimate use, least privilege, and separation of duties. Access control could be based on user identity, role, group membership, or other information known to the system.

Most operating systems and some applications provide some authentication and authorization functionality. For example, user identification (ID) codes and passwords are the most commonly used authentication technology. System administrators can assign users rights and privileges to applications and data files based on user IDs. Some operating systems allow for the grouping of users to simplify the

administration of groups of users who require the same levels of access to files and applications.

Boundary Protection: Firewalls

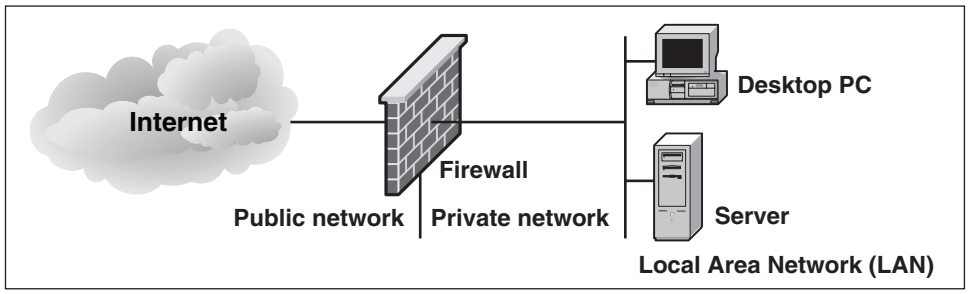
What the technology does

Firewalls are network devices or systems running special software that control the flow of network traffic between networks or between a host and a network. A firewall is set up as the single point through which communications must pass. This enables the firewall to act as a protective barrier between the protected network and any external networks. Any information leaving the internal network can be forced to pass through a firewall as it leaves the network or host. Incoming data can enter only through the firewall.

Firewalls are typically deployed where a corporate network connects to the Internet. However, firewalls can also be used internally, to guard areas of an organization against unauthorized internal access. For example, many corporate networks use firewalls to restrict access to internal networks that perform sensitive functions, such as accounting or personnel.

Personal computer users can also use firewalls, called personal firewalls, to protect their computers from unauthorized access over a network. Such personal firewalls are relatively inexpensive software programs that can be installed on personal computers to filter all network traffic and allow only authorized communications. Essentially, a firewall can be likened to a protective fence that keeps unwanted external data out and sensitive internal data in (see figure 10).

Figure 10: A Typical Firewall Protecting Hosts on a Private Network from the Public Network



Source: GAO analysis and Microsoft Visio.

How the technology works

Typically, a firewall is a network device or host with two or more network interfaces – one connected to the protected internal network and the other connected to unprotected networks, such as the Internet. The firewall runs software that examines the network packets arriving at its network interfaces and takes appropriate action based on a set of rules. The idea is to define these rules so that they allow only authorized network traffic to flow between the two interfaces. Configuring the firewall involves setting up the rules properly. A configuration strategy is to reject all network traffic and then enable only a limited set of network packets to go through the firewall. The authorized network traffic would include the connections necessary to perform functions such as visiting Web sites and receiving electronic mail.

NIST describes eight kinds of firewall platforms: packet filter firewalls, stateful inspection firewalls, application proxy gateway firewalls, dedicated proxy firewalls, hybrid firewall technologies, network address translation, host-based firewalls, and personal firewalls/personal firewall appliances.[2]

Packet filter firewalls are routing devices that include access control functionality for system addresses and communication sessions. The access control functionality of a packet filter firewall is governed by a set of rules that allows or blocks network packets based on a number of their characteristics, including the source and destination addresses, the

[2]National Institute of Standards and Technology, *Guidelines for Firewalls and Firewall Policy*, NIST Special Publication 800-41, (Gaithersburg, MD: Jan. 2002).

network protocol, and the source and destination port numbers. Packet filter firewalls are usually placed at the outermost boundary with an untrusted network, and they form the first line of defense. An example of a packet-filter firewall is a network router that employs filter rules to screen network traffic.

Stateful inspection firewalls keep track of network connections that are used by network applications to reliably transfer data. When an application uses a network connection to create a session with a remote host system, a port is also opened on the originating system. This port receives network traffic from the destination system. For successful connections, packet filter firewalls must permit inbound packets from the destination system. Opening up many ports to incoming traffic creates a risk of intrusion by unauthorized users, who may employ a variety of techniques to abuse the expected conventions of network protocols such as TCP. Stateful inspection firewalls solve this problem by creating a directory of outbound network connections, along with each session's corresponding client port. This "state table" is then used to validate any inbound traffic. The stateful inspection solution is more secure than a packet filter because it tracks client ports individually rather than opening all inbound ports for external access.

Application proxy gateway firewalls provide additional protection by inserting the firewall as an intermediary between internal applications that attempt to communicate with external servers such as a Web server. For example, a Web proxy receives requests for external Web pages from inside the firewall and relays them to the exterior Web server as though the firewall was the requesting Web client. The external Web server responds to the firewall and the firewall forwards the response to the inside client as though the firewall was the Web server. No direct network connection is ever made from the inside client host to the external Web server.

Dedicated proxy servers are typically deployed behind traditional firewall platforms. In typical use, a main firewall might accept inbound network traffic, determine which application is being targeted, and then hand off the traffic to the appropriate proxy server (for example, an e-mail proxy server). The proxy server typically would perform filtering or logging operations on the traffic and then forward it to internal systems. A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and then pass it to the firewall for outbound delivery. Many organizations enable the caching of frequently used Web pages on the proxy server, thereby reducing firewall traffic. In

addition to authentication and logging functionality, dedicated proxy servers are useful for Web and electronic mail content scanning.

Hybrid firewall technologies are firewall products that incorporate functionality from several different types of firewall platforms. For example, many vendors of packet filter firewalls or stateful inspection packet filter firewalls have implemented basic application-proxy functionality to offset some of the weaknesses associated with their firewall platform. In most cases, these vendors implement application proxies to provide improved logging of network traffic and stronger user authentication. Nearly all major firewall vendors have introduced multiple firewall functions into their products in some manner; therefore it is not always a simple matter to decide which specific firewall product is the most suitable for a given application or enterprise infrastructure. Selection of a hybrid firewall product should be based on the supported feature sets that an enterprise needs.

Network address translation (NAT) technology is an effective tool for "hiding" the network addresses of an internal network behind a firewall environment. In essence, NAT allows an organization to deploy a network addressing plan of its choosing behind a firewall while still maintaining the ability to connect to external systems through the firewall. Network address translation is accomplished by one of three methods: static, hiding, and port. In static NAT, each internal system on the private network has a corresponding external, routable IP address associated with it. This particular technique is seldom used because unique IP addresses are in short supply. With hiding NAT, all systems behind a firewall share the same external, routable IP address, while the internal systems use private IP addresses. Thus, with a hiding NAT system, a number of systems behind a firewall will still appear to be a single system. With port address translation, it is possible to place hosts behind a firewall system and still make them selectively accessible to external users.

Host-based firewalls are firewall software components that are available in some operating systems or as add-ons. Because a network-based firewall cannot fully protect internal servers, host-based firewalls can be used to secure individual hosts.

Personal firewalls and personal firewall appliances are used to secure PCs at home or remote locations. These firewalls are important because many personnel telecommute or work at home and access sensitive data. Home users dialing an ISP may potentially have limited firewall protection available to them because the ISP has to accommodate

many different security policies. Therefore, personal firewalls have been developed to provide protection for remote systems and to perform many of the same functions as larger firewalls. These products are typically implemented in one of two configurations. The first configuration is a personal firewall, which is installed on the system it is meant to protect; personal firewalls usually do not offer protection to other systems or resources. Likewise, personal firewalls do not typically provide controls over network traffic that is traversing a computer network—they protect only the computer system on which they are installed. The second configuration is a personal firewall appliance. In most cases, personal firewall appliances are designed to protect small networks such as networks that might be found in home offices. These appliances usually run on specialized hardware and integrate some other form of network infrastructure components in addition to the firewall itself, including the following: cable or digital subscriber line broadband modem with network routing, network hub, network switch, DHCP server, SNMP agent, and application-proxy agents. In terms of deployment strategies, personal firewalls and personal firewall appliances normally address connectivity concerns associated with telecommuters or branch offices. However, some organizations employ these devices on their organizational intranets, practicing a layered defense strategy.

Centrally managed distributed firewalls are centrally controlled but locally enforced. A security administrator— not the end users—defines and maintains security policies. This places the responsibility and capability of defining security policies in the hands of a security professional who can properly lock down the target systems. A centrally managed system is scalable because it is unnecessary to administer each system separately. A properly executed distributed firewall system includes exception logging. More advanced systems include the capability to enforce the appropriate policy, which is enforced depending on the location of the firewall. Centrally managed distributed firewalls can be either software- or hardware-based firewalls. Centrally managed distributed software firewalls are similar in function and features to host-based or personal firewalls, but the security policies are centrally defined and managed. Centrally managed distributed hardware firewalls combine the filtering capability of a firewall with the connectivity capability of a traditional connection.

Effectiveness of the technology

When properly configured, all firewalls can protect a network or a PC from unauthorized access through the network. Although firewalls afford protection of certain resources within an organization, there are some threats that firewalls cannot protect against: connections that bypass the

firewall, new threats that have not yet been identified, and viruses that have been injected into the internal network. It is important to consider these shortcomings in addition to the firewall itself in order to counter these additional threats and provide a comprehensive security solution. Each type of firewall platform has its own strengths and weaknesses.

Packet filter firewalls have two main strengths: speed and flexibility. Packet filter firewalls can be used to secure nearly any type of network communication or protocol. This versatility allows packet filter firewalls to be deployed into nearly any enterprise network infrastructure. Packet filter firewalls have several weaknesses: They cannot prevent attacks that exploit application-specific vulnerabilities or functions; they can log only a minimal amount of information, such as source address, destination address, and traffic type; they do not support user authentication; and they are vulnerable to attacks and exploits that take advantage of flaws within the TCP/IP protocol, such as IP address spoofing.[3]

Stateful inspection firewalls share the strengths and weaknesses of packet filter firewalls, but because of the state table implementation, they are generally considered to be more secure than packet filter firewalls. Stateful inspection firewalls can accommodate other network protocols in the same manner as packet filters do, but stateful inspection technology is relevant only to the TCP/IP protocol.

Application-proxy gateway firewalls have numerous advantages over packet filter firewalls and stateful inspection firewalls. First, application-proxy gateway firewalls are able to examine the entire network packet rather than only the network addresses and ports. This enables these firewalls to provide more extensive logging capabilities than packet filters or stateful inspection firewalls. Another advantage is that application-proxy gateway firewalls can authenticate users directly, while packet filter firewalls and stateful inspection firewalls normally authenticate users based on the network address of the system (i.e., source, destination, and type). Given that network addresses can be easily spoofed, the authentication capabilities inherent in application-proxy gateway architecture are superior to those found in packet filter or stateful inspection firewalls. The advanced functionality of application-proxy gateway firewalls also results in several disadvantages when compared

[3]IP address spoofing involves altering the address information in network packets in order to make packets appear to come from a trusted IP address.

with packet filter or stateful inspection firewalls. First, because of the "full packet awareness" found in application-proxy gateways, the firewall is forced to spend significant time reading and interpreting each packet. Therefore, application proxy gateway firewalls are generally not well suited to high-bandwidth or real-time applications. To reduce the load on the firewall, a dedicated proxy server can be used to secure less time-sensitive services, such as e-mail and most Web traffic. Another disadvantage is that application proxy gateway firewalls are often limited in terms of support for new network applications and protocols. An individual, application-specific proxy agent is required for each type of network traffic that needs to go through the firewall. Most vendors of application-proxy gateways provide generic proxy agents to support undefined network protocols or applications. However, those generic agents tend to negate many of the strengths of the application-proxy gateway architecture, and they simply allow traffic to "tunnel" through the firewall.

Dedicated proxy servers allow an organization to enforce user authentication requirements and other filtering and logging of any traffic that goes through the proxy server. This means that an organization can restrict outbound traffic to certain locations, examine all outbound e-mail for viruses, or restrict internal users from writing to the organization's Web server. Because most security problems originate from within an organization, proxy servers can assist in foiling internally based attacks or malicious behavior.

In terms of strengths and weaknesses, each type of NAT—static, hiding, or port—is applicable in certain situations; the variable is the amount of design flexibility offered by each type. Static NAT offers the most flexibility, but it is not always practical because of the shortage of IP addresses. Hiding NAT technology is seldom used because port address translation offers additional features. Port address translation is often the most convenient and secure solution.

Host-based firewall packages typically provide access-control capability for restricting traffic to and from servers that run on the host, and logging is usually available. A disadvantage of host-based firewalls is that they must be administered separately, and maintaining security becomes more difficult as the number of configured devices increases.

Centrally managed distributed software firewalls have the benefit of unified corporate oversight of firewall implementation on individual machines. However, they remain vulnerable to attacks on the host

operating system from the networks, as well as to intentional or unintentional tampering by users logging in to the system that is being protected. Centrally managed distributed hardware firewalls filter the data on the firewall hardware rather than the host system. This can make the distributed hardware firewall system less vulnerable than software-based distributed firewalls. Hardware distributed firewalls can be designed to be unaffected by local or network attacks via the host operating systems. Performance and throughput of a hardware firewall system are generally better than they are for software systems.

Boundary Protection: Content Management

What the technology does

Content filters monitor Web and messaging applications for inappropriate content, spam, intellectual property breach, non-compliance with an organization's security policies, and banned file types.[4] The filters can help to keep illegal material out of an organization's systems, reduce network traffic from spam, and stop various forms of cyber attacks. They can also keep track of which users are browsing the Web, when, where, and for how long.

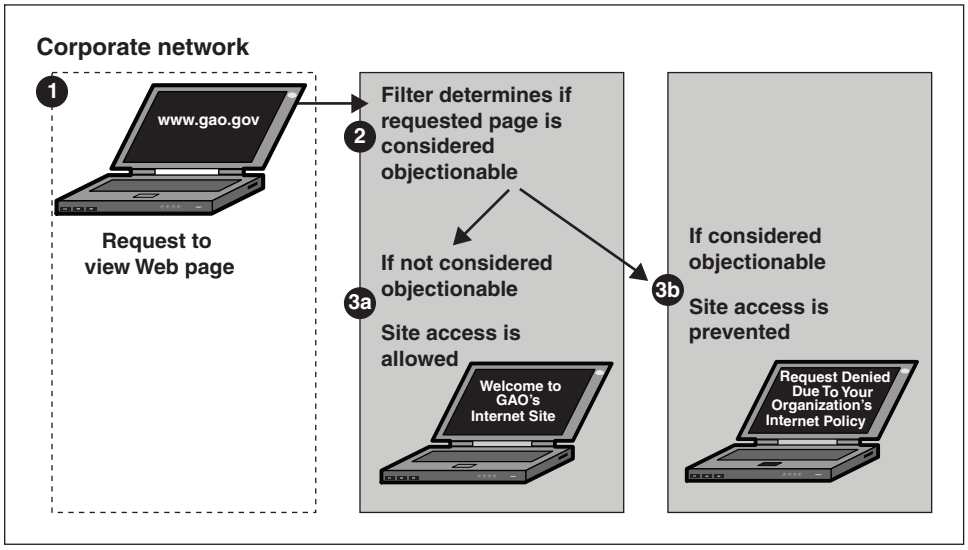
There are three main types of content filters: (1) Web filters, which screen and exclude from access or availability Web pages that are deemed objectionable or non-business related; (2) messaging filters, which screen messaging applications such as e-mail, instant messaging, short message service, and peer-to-peer service for spam or other objectionable content;[5] and (3) Web integrity filters, which ensure the integrity of an entity's Web pages.

[4]Spam is electronic junk mail that is unsolicited and usually is advertising for some product. An intellectual property breach can include client information, trade secrets, ongoing research, and other such information that has been released without authorization.

[5]Short message service is the transmission of short text messages to and from a mobile phone, fax machine or IP address. Messages must be no longer than 160 alphanumeric characters and contain no images or graphics. On the Internet, peer-to-peer (referred to as P2P) networks allow computer users to share files from one another's hard drives. Napster, Gnutella, and Kazaa are examples of this kind of peer-to-peer software.

How the technology works

Figure 11: How a Web Filter Works



Source: GAO analysis and Microsoft Visio.

Web filters screen and block objectionable Web pages by (1) intercepting a user's request to view a Web page, (2) determining that the requested page contains objectionable content, and (3) prohibiting the user from accessing that Web page (see figure 11). Web filters can observe and respond to requests in two main ways. One method, pass-through technology, requires the Web filtration software to be integrated with other network devices such as proxies or gateways. This ensures that all requests pass through the Web filter to be accepted or denied. Another method of handling requests, known as pass-by technology, requires the Web filtration software to be installed on a stand-alone server and placed on the network of machines that it is to filter. The Web filter then receives all of the traffic that exists on the network, but it does not prevent the network traffic from reaching its intended destination. If a request is made for a restricted Web page, the Web filter will display an error message stating that the user's access to the Web page was denied. The user's connection with the Web site is then closed to prevent the Web server from sending additional information to the user's computer. Web filters also vary in their methods of determining if a requested Web page contains objectionable material:

- **Site classification** technology compares the requested Web site against a database of Web pages that are considered objectionable.

Typically, vendors provide a basic database of objectionable Web pages as part of the Web filter software, which may then be modified by an administrator. Vendors often provide subscription services so customers' databases can be automatically updated with new sites that were found to be objectionable. The database consists primarily of a list of Web site addresses, typically categorized into groups such as gambling, adult material, and sports. An administrator can then decide which sites should be blocked, based on the category they fall into. If the requested Web site is on the list of objectionable Web sites, the Web filter will display a message informing the user that he or she has been denied access to the Web page.

- **Content classification** uses artificial intelligence in conjunction with site classification techniques to maintain an updated database. Before a user can view a Web site, the Web filter examines the textual content of the Web page, the source code, and metatags.[6] Questionable content is identified by the presence of key words or phrases or by a combination of key word frequency and level of obscenity of the words. Web sites found to be objectionable, based on the content, can then be added into the database of objectionable sites, and the user would not be allowed to view them. Web sites do not have to be blocked for an entire organization, but can be blocked based on IP address ranges, host names, or other criteria.

Messaging filters operate similarly to Web filters, and can examine the content of a message to filter out spam, offensive language, or recreational e-mails that lower the productivity of workers. Messaging filters also block messages based on the types of file attachments and the senders of e-mails, as determined by an organization's policy. Files are excluded based on their file extensions, or the last part of their name, which indicates the file type. The file might be excluded to limit the trafficking of illicit material, stop viruses from entering the network, limit intellectual property breaches, or carry out other such functions intended to increase the security of an organization. File extensions that are typically excluded are MP3 (music files), JPG (graphic files), MPEG (video files), and EXE (typically used for executable files), among others.

[6]The source code is the text of a program while it is still in its programming language. The Hypertext Markup Language (HTML) metatag is used to describe the contents of a Web page

A Web integrity filter ensures the integrity of the content of a Web page. If a Web server is attacked or becomes inaccessible to users, the Web integrity filter attempts to keep unauthorized information from being released to the public, and only the original content would still go out. The content filter is a separate device on the network, located between the Web server and the router or firewall. The device contains a collection of digital signatures of authorized Web content that is known to be legitimate. When a request is made to the Web server, each object's[7] digital signature is compared with the digital signature that the device had previously collected. If the digital signatures do not match, the page is considered to be unauthorized and it is immediately replaced with a secure archived copy of the original pages, and the software notifies the appropriate personnel via phone, e-mail or pager.

Effectiveness of the technology

Content filters have significant rates of both erroneously accepting objectionable sites and of blocking sites that are not objectionable. If implemented correctly, filtering can reduce the volume of unsolicited and undesired e-mails. However, it is not completely accurate, and legitimate messages might get blocked. Also, some content filters do not work with all operating systems.

While pass-through technology can be effective at stopping specified traffic, there are several disadvantages to using it. First, because the requests for Web sites are actually stopped at the gateway while the filtering product analyzes the request against its rules, a certain amount of latency can result, especially during periods of high traffic volume.[8] Second, pass-through products might be considered a single point of failure: If the product fails, so might Internet connectivity. Third, because pass-through devices are dependent on another network device, if an entity changes firewalls or proxy servers, it might have to purchase a new content filter product as well. Pass-by technology can also be effective at stopping specified traffic. Because traffic does not have to be screened before it goes through, the pass-by technology does not cause latency. Also, because pass-by products do not require integration with other network devices, a change in a firewall or proxy would not result in a need to change the content filtering product. However, a disadvantage of the

[7]An object can be an HTML page, a graphic file, a music file, and so forth.

[8]Latency is the amount of time it takes a packet to travel from source to destination. Together, latency and bandwidth define the speed and capacity of a network.

pass-by solution is that a separate server must be dedicated to performing the monitoring and filtering functions.

Site classification is effective at keeping users from accessing sites that have been determined to have objectionable content. However, because of the size and growth of the Internet, this technology faces difficulties in keeping a full and accurate list of objectionable sites, and the cost of subscriptions for updates can be very expensive. Content classification can assist in classifying new sites without the cost of subscribing to an update service, but this method has its drawbacks as well. First, Web sites that are predominantly graphical in nature may not contain enough key words for the program to categorize the site. Second, there are some topics that are so ambiguous that it is very difficult to classify them by their content. Third, users may circumvent the filtered lists by using proxy sites.

Authentication: Biometrics

What the technology does

The term *biometrics* covers a wide range of technologies that are used to verify identity by measuring and analyzing human characteristics. Biometric technologies are authentication techniques that rely on measuring and analyzing physiological or behavioral characteristics. Identifying an individual's physiological characteristic involves measuring a part of the body, such as fingertips or eye irises; identifying behavioral characteristics involves data derived from actions, such as speech.

Biometrics are theoretically very effective personal identifiers because the characteristics they measure are thought to be distinct to each person. Unlike conventional identification methods that use something you have (for example, a smart card), or something you know (for example, a password), these characteristics are integral to something you are. Because they are tightly bound to an individual, they are more reliable, cannot be forgotten, and are less easily lost, stolen, or guessed.

How the technology works

Although biometric technologies vary in complexity, capabilities, and performance, they all share several elements. Biometric identification systems are essentially pattern recognition systems. They use acquisition devices such as cameras and scanning devices to capture images, recordings, or measurements of an individual's characteristics, and they use computer hardware and software to extract, encode, store, and compare these characteristics. Because the process is automated, biometric decision making is generally very fast, in most cases taking only

a few seconds in real time. The different types of biometric technologies measure different characteristics. However, they all involve a similar process, which can be divided into two distinct stages: (1) enrollment and (2) verification or identification.

Enrollment stage. Acquisition devices such as cameras and scanners are used to capture images, recordings, or measurements of an individual's characteristics, and computer hardware and software are used to extract, encode, store, and compare these characteristics. In the enrollment stage, the captured samples are averaged and processed to generate a unique digital representation of the characteristic, called a reference template, which is stored for future comparisons. It is impossible to recreate the sample, such as a fingerprint, from the template. Templates can be stored centrally on a computer database, within the device itself, or on a smart card.

Verification or identification stage. Depending on the application, biometric technologies can be used in one of two modes: verification or identification. Verification is used to verify a person's identity, answering the question "Is this person who she claims to be?" Identification is used to establish a person's identity, comparing the individual's biometric with all stored biometric records to answer the question "Who is this person?"

Current biometric technologies that are used to protect computer systems from unauthorized access include fingerprint recognition, iris recognition, and speaker recognition. These technologies are used by some entities to replace passwords as a way to authenticate individuals who are attempting to access computers and networks

Fingerprint recognition technology extracts features from impressions that are made by the distinctive ridges on the fingertips. An image of the fingerprint is captured by a scanner, enhanced, and converted into a template. Various styles of fingerprint scanners are commercially available. The scanner can be built into the computer or into the mouse or the keyboard that are attached to the computer, or it can be a hardware device that is used only for capturing fingerprints (see figures 12 and 13).

Figure 12: An Example of Fingerprint Recognition Technology Built into a Keyboard

Source: Key Tronic Corporation.

Figure 13: An Example of Fingerprint Recognition Technology Built into a Mouse

Source: Siemens PSE TechLab.

Iris recognition technology is based on the distinctly colored ring surrounding the pupil of the eye. Made from elastic connective tissue, the iris is a very rich source of biometric data, having approximately 266 distinct characteristics. Iris recognition systems use a small, high-quality camera to capture a black-and-white, high-resolution image of the iris. The boundaries of the iris are defined and a coordinate system is established over the iris before visible characteristics are converted into a template (see figure 14).

Figure 14: A Desktop Iris Recognition System

Source: Matsushita Electric Corporation of America.

Speaker recognition technology uses the distinctive characteristics in the sound of people's voices as a biometric identifier. These differences result from a combination of physiological differences in the shape of vocal tracts and learned speaking habits. Speaker recognition systems capture samples of a person's speech by having him or her speak into a microphone or telephone a number of times. Some systems require that a predefined phrase, such as a name or a sequence of numbers, be used for enrollment. This phrase is converted from analog to digital format, and the distinctive vocal characteristics, such as pitch, cadence, and tone, are extracted to create a template.

Effectiveness of the technology

The quality of templates is critical in the overall success of a biometric system. Minute changes in positioning, distance, pressure, environment, and other factors influence the generation of a template. For example, in a speaker recognition system, performance can be affected by background noise, the use of different capture devices for enrollment and verification,

speaking softly, and poor placement of the capture device. In addition, because biometric features can change over time, people may have to re-enroll to update their reference templates.

Furthermore, not all people can use biometric technologies. For example, the capturing of fingerprints for about 2 to 5 percent of people is not possible because the fingerprints are dirty or have become dry or worn from age, extensive manual labor, or exposure to corrosive chemicals. People who are mute cannot use speaker recognition systems, and people lacking fingers or eyes from congenital disease, surgery, or injury cannot use fingerprint or iris recognition systems.

The effectiveness of biometric technologies is affected by the quality of the capture device. For example, some fingerprint recognition scanners can be prone to error if there is a buildup of dirt, grime, or oil—producing leftover fingerprints from previous users, which are known as latent prints. Severe latent prints can cause the superimposition of two sets of prints and degrade the capturing of the image. Similarly, the performance of speaker recognition systems improves with higher-quality input devices.

Tests have shown that certain capture devices can be tricked into accepting forgeries. Fingerprint scanners have been tricked into accepting latent prints that were reactivated by simply breathing on the sensor or by placing a water-filled plastic bag on the sensor's surface. It is possible to reconstruct and authenticate latent fingerprints by dusting the sensor's surface with commercially available graphite powder and lifting the fingerprint with adhesive tape. A vulnerability of speaker authentication is that the voice can be easily recorded and therefore duplicated. However, some speaker verification systems provide safeguards against the use of a recorded voice to trick the system. For these systems, the electronic properties of a recording device, particularly the playback speaker, will change the acoustics to such a degree that the recorded voice sample will not match a stored voiceprint of a live voice.

Authentication: Smart Tokens

What the technology does

A smart token is an easily portable device that contains an embedded integrated circuit chip that is capable of both storing and processing data. Most smart tokens are used instead of static user IDs and passwords to provide a stronger and more convenient means for users to identify and authenticate themselves to computers and networks. When it is used for

this function, a smart token is an example of authentication based on something a user possesses (for example, the token itself). Although authentication to some computer systems is based solely on the possession of a token, typical smart token implementations also require a user to provide something he or she knows (for example, a password) in order to successfully utilize the smart token.

How the technology works

In general, smart tokens can be classified according to physical characteristics, interfaces, and protocols used. These classifications are not mutually exclusive.

1. **Physical characteristics.** Smart tokens can be divided into two physical groups: smart cards and other tokens. A smart card looks like a credit card but includes an embedded microprocessor. Smart tokens that are not smart cards can look like calculators, keys, or other small objects.

2. **Interfaces**. Smart tokens have either a human or an electronic interface. Smart tokens that look like calculators usually have a human interface, which allows humans to communicate with the device. Other smart tokens, including smart cards, have an electronic interface that can only be understood by special readers and writers. Two physical interfaces for smart cards have been standardized through the International Organization for Standardization, resulting in two types of smart cards. The first type, known as contact cards, works by inserting the card in a smart card reader, while the second type, known as contactless cards, uses radio frequency signals and the card needs only to be passed within close proximity to a card terminal to transmit information. Smart cards can be configured to include both contact and contactless capabilities, but because standards for the two technologies are very different, two separate interfaces would be needed.

3. **Protocols**. Smart tokens use three main methods for authentication, based on different protocols. The first method, static password exchange, requires users to first authenticate themselves to a token before the token can then authenticate the user to the computer. The other two methods are known as time-synchronized and challenge-response, and are based on cryptography. These methods generate a one-time password, which is a password or pass code that can be used only once, for a brief interval, and then is no longer valid. If it is intercepted in any way, the password has such a limited life span that it quickly becomes invalid. The next time the same user attempts to

access a system, he or she must enter a new one-time password that is generated by the security token.

Time-synchronized tokens generate a unique value that changes at regular intervals (for example, once a minute). A central server keeps track of the token-generated passwords in order to compare the input against the expected value. To log onto a system, users enter a one-time password that consists of their personal PIN followed by the unique value generated by their token. The PIN helps the central server to identify the user and the password value that should be entered. If the number entered by the user and the one generated by the server are the same, the user will be granted access to the system. Figure 15 shows an example of a time-synchronized token.

Figure 15: Example of a Time-Synchronized Token

Source: RSA Security Inc.

Challenge-response tokens utilize a central server to generate a challenge (such as a random string of numbers), which a user would then enter into the token. The token then calculates a response that serves as a one-time numeric password that is entered into the system. If the response from the user is the same as the response expected by the server, the user will be granted access to the system. In some implementations, the user must enter a PIN before the server will generate a challenge. Figure 16 illustrates an example of a challenge-response token.

Figure 16: Example of a Challenge-Response Token

Source: © 2004 Secure Computing Corporation.

Universal Serial Bus (USB) tokens are slender tokens with USB connectors that plug into PCs' USB ports. The token has an integrated chip that offers the same storage and processing power as smart cards. USB tokens can be used to securely store a user's private keys and, optionally, to securely perform cryptographic processing. A USB token can also securely store many user names and passwords, with the benefit of portability and additional security of off-PC storage.

Effectiveness of the technology

If they are implemented correctly, smart tokens can help create a secure authentication environment. Onetime passwords eliminate the problem of electronic monitoring or "password sniffing" and tokens that require the use of a PIN help to reduce the risk of forgery.

However, smart tokens do not necessarily verify a person; they only confirm that a person has the token. Because tokens can be lost or stolen, an attacker could obtain a token and attempt to determine the user's PIN or password. If an older algorithm is used to formulate a onetime password, it is possible that modern computers could crack the algorithm used to formulate the random numbers generated by a token. For these reasons, these technologies are generally not considered acceptable as stand-alone systems to protect extremely sensitive data, and additional controls—such as biometric identification—may be required. As a result, smart token systems are considered more effective when combined with other methods of authentication.

In addition, at times the token could become unavailable to the user. For example, tokens can be broken, their batteries eventually discharge, and

users could simply forget to bring tokens to work. For these reasons, organizations need to have an effective policy on how legitimate users can access systems without a token. If the policy is weak or poorly implemented, the security of the authentication system is weakened.

A problem that can arise with time-synchronized tokens is that the token and the central authentication server can get out of sync. If the token's clock drifts significantly ahead of or behind the server's clock, the authentication server may be vulnerable to a cryptographic attack.

Authorization: User Rights and Privileges

What the technology does

User rights and privileges grant or deny access to a protected resource, whether it is a network, system, an individual computer, a program, or a file. These technologies authorize appropriate actions for users and prevent unauthorized access to data and systems. Typically, user rights and privileges are capabilities that are built into an operating system. For example, most operating systems include the concept of read, write, or read-and-write privileges for files and the capability to assign these privileges to users or groups of users.

Mainframe-based access control software controls users' entry to the system, their access to data on the system, and the level of usage available to them with programs and other logical resources that are on the system. Administrators can use these software tools to perform many access control functions—including identifying system users and authorizing user access to protected resources—while also ensuring individual accountability and logging unauthorized attempts at gaining access to the system protected resources.

Additionally, some communication protocols can be used to control dial-up access into networks. Protocols that provide these services include Terminal Access Controller Access System (TACACS+), which centrally manages multiple connections to a single user, a network, or a subnetwork, and interconnected networks, and Remote Authentication Dial-In User Service (RADIUS), which provides central authentication, authorization, and logging.

How the technology works

Mainframe-based access control software uses algorithms to determine whether to grant a user access to specific files, programs, or other defined resources (such as a printer queue or disk space to run a program). These

algorithms are typically customized by a security administrator and result in access rules that are either user- or resource-based. User-based rules can be created to specify access for individuals or for groups. When access is requested, the software first identifies and authenticates the user, then determines what resource the user is requesting access to, and then refers to the access rules before permitting the user to gain access to protected system resources. Access is denied to unauthorized users, and any authorized or unauthorized attempt to gain access can be logged.

Technologies that use resource-based rules assign a security classification to both users and data files in the form of security levels and categories. The levels and categories of a user and a resource are compared to determine whether the user has sufficient privileges to access a file or other resource.

The TACACS+ protocol allows a separate access server to independently provide the services of authentication, authorization, and accounting. The authentication service allows a user to use the same user name and password for multiple servers, which may employ different communication protocols: TACACS+ forwards the user's user name and password information to a centralized database that also has the TACACS+ protocol. This database then compares the login information to determine whether to grant or deny access to the user.

RADIUS is implemented in a client/server network architecture, where a centralized server using the RADIUS protocol maintains a database of all user authentication and network service access information for several client computers that also use the RADIUS protocol. When a user logs on to the network via a RADIUS client, the user's password is encrypted and sent to the RADIUS server along with the user name. If the user name and password are correct, the server sends an acknowledgement message that includes information on the user's network system and service requirements. If the login process conditions are met, the user is authenticated and is given access to the requested network services.

Effectiveness of the technology

An operating system's built-in user rights and privileges can be effective when used with a well-defined security policy that guides who can access which resources.

A key component to implementing adequate access controls is ensuring that appropriate user rights and privileges have been assigned. If any one user has too many rights or has rights to a few key functions, the organization can be susceptible to fraud. Limiting user rights and

privileges ensures that users have only the access they need to perform their duties, that very sensitive resources are limited to a few individuals, and that employees are restricted from performing incompatible functions or functions that are beyond their responsibilities. Excluding roles and user rights reduce the possibility of fraudulent acts against the organization.

System Integrity

System integrity technologies are used to ensure that a system and its data are not illicitly modified or corrupted by malicious code. Malicious code includes viruses, Trojan horses, and worms. A virus is a program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when a user takes some action, such as opening an infected e-mail attachment or executing a downloaded file that includes the virus. When executed, the virus can infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate. A Trojan horse is a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. A worm is an independent computer program that reproduces by copying itself from one system to another. Unlike a computer virus, a worm does not require human involvement to propagate.

Antivirus software and integrity checkers are two types of technologies that help to protect against malicious code attacks. Antivirus software can be installed on computers to detect either incoming malicious code or malicious code that is already resident on the system and to repair files that have been damaged by the code. Integrity checkers are usually applied to critical files or groups of files on a computer system. These programs typically take a snapshot of the files of interest and periodically compare the files with the snapshot to ensure that no unauthorized changes have been made.

Antivirus Software

What the technology does

Antivirus software provides protection against viruses and malicious code, such as worms and Trojan horses, by detecting and removing the malicious code and by preventing unwanted effects and repairing damage that may have resulted. Antivirus software uses a variety of techniques—such as signature scanners, activity blockers, and heuristic scanners—to protect computer systems against potentially harmful viruses, worms, and Trojan horses.

How the technology works

Antivirus software products can use a combination of the following technologies:

Signature scanners can identify known malicious code. Scanners search for "signature strings" or use algorithmic detection methods to identify known code. They rely on a significant amount of prior knowledge about the malicious code. Therefore, it is critical that the signature information for scanners be current. Most scanners can be configured to automatically update their signature information from a designated source, typically on a weekly basis; scanners can also be forced to update their signatures on demand.

Activity (or behavior) blockers contain a list of rules that a legitimate program must follow. If the program breaks one of the rules, the activity blockers alert the users. The idea is that untrusted code is first checked for improper behavior. If none is found, the code can be run in a restricted environment, where dynamic checks are performed on each potentially dangerous action before it is permitted to take effect. By adding multiple layers of reviews and checks to the execution process, behavior blockers can prevent malicious code from performing undesirable actions.

Heuristic scanners work to protect against known viruses and are also able to detect unknown viruses. Heuristic scanners can be classified as either static or dynamic. Static heuristic scanners use virus signatures, much like standard signature scanners, but instead of scanning for specific viruses, they scan for lines of code that are associated with viruslike behaviors. These scanners are often supplemented by additional programs that search for more complex, viruslike behavior patterns. Dynamic heuristic scanners identify suspicious files and load them into a simulated computer system to emulate their execution. This allows the scanner to determine if the file is infected.

Effectiveness of the technology

Signature scanners require frequent updates to keep their databases of virus signatures current. This updating is necessary to safeguard computer systems against new strains of viruses. When they are properly updated, scanners effectively combat known viruses. However, they are less effective against viruses that change their code each time they infect another computer system.

Activity blockers are generally ineffective against many viruses, including macro viruses that make use of the programming features of common applications such as spreadsheets and word processors. Macro viruses

constitute the majority of today's viruses and are encoded within a document as macros—sequences of commands or keyboard strokes that can be stored and then recalled with a single command or keystroke. The macro generally modifies a commonly used function (for example, opening or saving a file) to initiate the effect of the virus. Activity blockers are generally more successful against Trojan horses and worms than they are against viruses.

Heuristic scanners have the primary advantage of being able to detect unknown viruses. Static heuristic scanners, when supplemented with additional programs that can detect behaviors associated with more complex viruses. Dynamic heuristic scanners consume more time and system resources than static heuristic scanners.

File Integrity Checkers

What the technology does

File integrity checkers are software programs that monitor alterations to files that are considered critical to either the organization or the operation of the computer (including changes to the data in the file, permissions, last use, and deletion). Because both authorized and unauthorized activities alter files, file integrity checkers are designed for use with critical files that are not expected to change under normal operating conditions.

File integrity checkers are valuable tools with multiple uses, including

- **Intrusion detection**. File integrity checkers can help detect system compromises because successful intruders commonly modify system files to provide themselves with a way back into the system (backdoor), hide the attack, and hide their identity.
- **Administration**. Some file integrity checkers have the ability to collect and centralize information from multiple hosts, an ability that assists system administrators in large network environments.
- **Policy enforcement**. System administrators can use file integrity checkers as a policy enforcement tool to check whether users or other administrators have made changes that should not have been made or of which the system administrator was not notified.
- **Identification of hardware or software failure**. Integrity checkers might also notice a failing disk. File integrity checkers can also be used to determine if an application had changed files because of design faults.

- **Forensic analysis**. If a system were compromised, a "snapshot" of the system could be taken, which would assist forensic activities and in prosecuting offenders.

How the technology works

Integrity checkers identify modifications to critical files by comparing the state of a file system against a trusted state, or a baseline.[9] The baseline is set to reflect the system's state when it has not been modified in any unauthorized way. First, critical files are encrypted through a one-way hash function, making it nearly impossible to derive the original data from the string.[10] The hash function results in a fixed string of digits, which are stored in a database along with other attributes of the files. The database of the original state of critical files is considered the baseline. To be effective, a baseline should be established immediately after the operating system is installed, before an attacker would have the ability to modify the file system.

After a baseline is created, the integrity checker can then compare the current file system against the baseline. Each critical file's hash is compared with the its baseline value. Differences between the hashes indicate that the file has been modified. The user can then determine if the change would have been unauthorized. If so, the user can take action, for example, assessing the damage and restoring the file or system to a good known state.

Effectiveness of the technology

The effectiveness of file integrity checkers depends on the accuracy of the baseline. Comparisons against a corrupted baseline would result in inaccuracy in identifying modified files. The baseline database should be updated whenever significant changes are made to the system. Care must be taken to ensure that a baseline is not taken of a compromised system.

Also, although they monitor modifications to files, integrity checkers do not prevent changes from occurring. An administrator will notice that the change has occurred only after the integrity checker has been run. Because of the amount of time it can take to check a file system and the

[9]The file system is one of the most important parts of an operating system; and it stores and manages user data on disk drives and ensures that data read from storage are identical to the data that were originally written. In addition to storing user data in files, the file system creates and manages metadata—information about how, when, and by whom a particular set of data was collected and how the data are formatted.

[10]A less secure method uses checksums instead of a hash function.

system resources that requires, these tools are typically run at regularly scheduled intervals.

In addition, integrity checkers may generate false alarms when authorized changes are made to monitored files. Not only can investigating false alarms be time-consuming, it could also lead a system administrator to be unwilling to investigate future alarms. As a result, unauthorized changes could go unnoticed.

Cryptography

Cryptography is used to secure transactions by providing ways to assure data confidentiality (assurance that the information will be protected from unauthorized access), data integrity (assurance that data have not been accidentally or deliberately altered), authentication of message originator, electronic certification of data, and nonrepudiation (proof of the integrity and origin of the data that can be verified by a third party). Accordingly, cryptography has had, and will continue to have, an important role in protecting information both within a computer system and when information is sent over the Internet and other unprotected communications channels. Encryption is the process of transforming ordinary data (commonly referred to as plaintext) into code form (ciphertext) using a special value known as a key and a mathematical process called an algorithm. Cryptographic algorithms are designed to produce ciphertext that is unintelligible to unauthorized users. Decryption of ciphertext is possible only with use of the proper key.

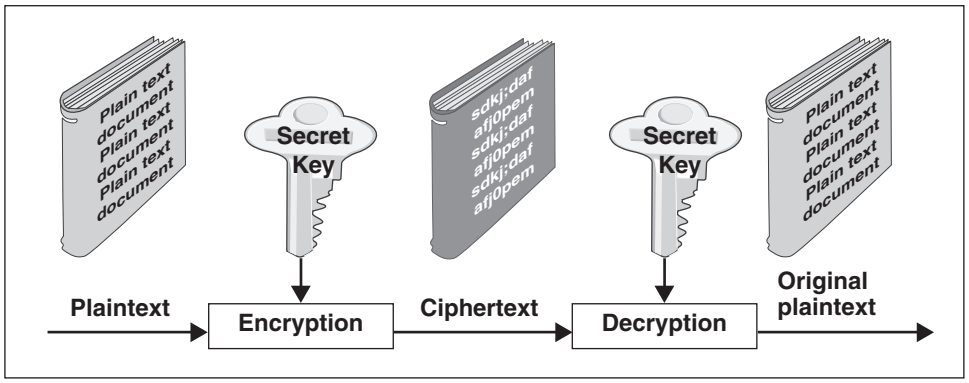
A basic premise in cryptography is that good systems depend only on the secrecy of the key used to perform the operations and not on the secrecy of the algorithm. The algorithms used to perform most cryptographic operations over the Internet are well known. However, because the keys used by these algorithms are kept secret, the process is considered secure.

Cryptographic techniques can be divided into two basic types: secret key cryptography and public key cryptography. Each type has its strengths and

weaknesses and systems that utilize both forms are used to take advantage of the strengths of a given type.[11]

- Secret key or symmetric cryptography employs algorithms in which the key that is used to encrypt the original plaintext message can be calculated from the key that is used to decrypt the ciphertext message, and vice versa. With most symmetric algorithms, the encryption key and the decryption key are the same, and the security of this method rests upon the difficulty of guessing the key. In order to communicate securely, the sender and the receiver must agree on a key and keep the key secret from others. Figure 17 depicts encryption and decryption using a symmetric algorithm. Common symmetric key algorithms include Triple Digital Encryption Standard (3DES) and the Advanced Encryption Standard (AES).

Figure 17: Encryption and Decryption with a Symmetric Algorithm



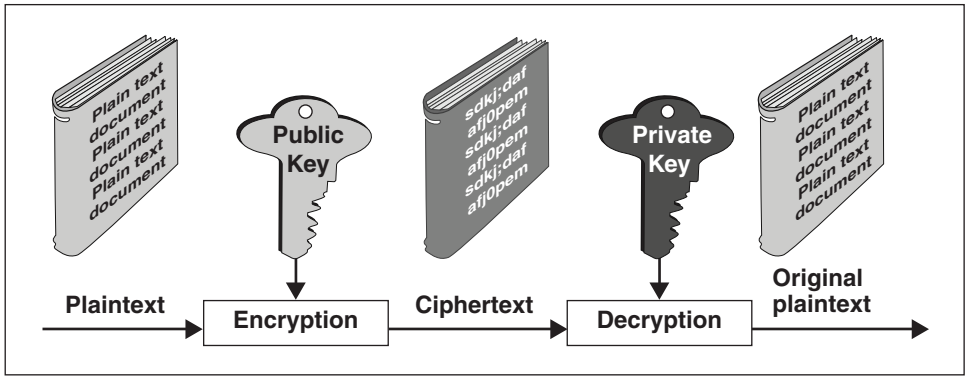
Source: GAO analysis and Corel Galley.

Public key or asymmetric cryptography employs algorithms designed so that the key that is used to encrypt the original plaintext message cannot be calculated from the key that is used to decrypt the ciphertext message. These two keys complement each other in such a way that when one key is used for encryption, only the other key can decrypt the ciphertext. One of these keys is kept private and is known as the *private key*, while the

[11]For additional information on how cryptography works and some of the issues associated with this technology see U.S. General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001), and U.S. General Accounting Office, *Information Security: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies*, GAO-04-157 (Washington, D.C.: Dec. 15, 2003).

other key is widely publicized and is referred to as the *public key*. Figure 18 depicts one application of encryption and decryption using a public key algorithm. In this process, the public key is used by others to encrypt a plaintext message, but only a specific person with the corresponding private key can decrypt the ciphertext. For example, if fictional character Bob gives his public key to fictional character Alice, only Bob has the private key that can decrypt a message that Alice has encrypted with his public key. Public key algorithms can also be used in an inverse process, whereby the private key is used to encrypt a message and the public key is made freely available. In this process, those who decrypt the message using the corresponding public key can be confident that the message came from a specific person. For example, if Alice decrypts a message that was encrypted with Bob's private key, she has assurance that the message came from Bob. The most popular public key algorithm is RSA, named for its creators—Rivest, Shamir, and Adleman.

Figure 18: Encryption and Decryption with a Public Key Algorithm



Source: GAO analysis and Corel Galley.

Key-based encryption fails if the plaintext or the key are not kept secret from unauthorized users. Such failures often occur not from a weakness in the technology itself, but rather as a result of poor security policies or practices or malicious insiders.

Secret key cryptography has significant limitations that can make it impractical as a stand-alone solution for securing electronic transactions, especially among large communities of users that may have no pre-established relationships. The most significant limitation is that some means must be devised to securely distribute and manage the keys that are at the heart of the system; such a means is commonly referred to as key management. When many transacting parties are involved, key

management may create immense logistical problems and delays. Furthermore, in order to minimize the damage that could be caused by a compromised key, the keys may need to be short-lived and therefore frequently changed, adding to the logistical complexity.

Public key cryptography can address many of the limitations of secret key cryptography regarding key management. There is no need to establish a secure channel or physical delivery services to distribute keys. However, public key cryptography has its own challenges, involving the methods of ensuring that the links between the users and their public keys are initially valid and are constantly maintained. For example, it is impractical and unrealistic to expect that each user will have previously established relationships with all of the other potential users in order to obtain their public keys. Digital certificates (discussed further in this appendix) are one solution to this problem. Furthermore, although a sender can provide confidentiality for a message by encrypting it with the recipient's publicly available encryption key using public key algorithms for large messages, this is computationally time-consuming and could make the whole process unreasonably slow.[12]

Instead, it can be better to combine secret and public key cryptography to provide more efficient and effective means by which a sender can encrypt a document so that only the intended recipient can decrypt it. In this case, the sender of a message would generate a onetime secret encryption key (called a session key) and use it to encrypt the body of her message and then encrypt this session key using the recipient's public key. The encrypted message and the encrypted session key necessary to decrypt the message would then be sent to recipient. Because the recipient has the information necessary to decrypt the session key, the sender of a message has reasonable assurance in a properly administered system that only the recipient would be able to successfully decrypt the message.

Cryptographic modules implement algorithms that form the building blocks of cryptographic applications. Using a cryptographic system with cryptographic modules that have been approved by an accredited cryptographic certification laboratory (for example, the NIST Cryptographic Module Validation Program) can help provide assurance

[12]Most public key cryptographic methods can be used for both encryption and digital signatures. However, certain public key methods—most notably the Digital Signature Algorithm—cannot be used for encryption, but only for digital signatures.

that the system will be effective. However, designing, building, and effectively implementing full-featured cryptographic solutions will remain a difficult challenge because it is more than just "installing the technology." Encryption technology is effective only if it is an integral part of an effectively enforced information security policy that includes good key management practices. For example, current public key products and implementations suffer from significant interoperability problems, which make it difficult for officials to make decisions about how to develop a public key infrastructure (PKI) that can be used to perform such functions as encrypting data and providing data integrity.[13]

Cryptographic solutions will continue to be used by systems to help provide the basic data confidentiality, data integrity, authentication of message originator, electronic certification of data, and nonrepudiation. Technologies that use cryptographic algorithms can be used to encrypt message transmissions so that eavesdroppers cannot determine the contents of the message. Hash technologies use cryptography to provide assurance to a message recipient that the contents of the message have not been altered. For example, operating systems use cryptography to protect passwords. Protocols such as IP Security protocol (IPSec) and Secure Sockets Layer (SSL) use cryptographic technologies for confidential communications. SHA and MD5 are examples of hash technology implementations. Digital signature technologies use cryptography to authenticate the sender of a message. Virtual private networks (VPN) use cryptography to establish a secure communications link across unprotected networks.

Digital Signatures and Certificates

What the technology does

Properly implemented digital signatures use public key cryptography to provide authentication, data integrity, and nonrepudiation for a message or transaction. Just as a physical signature provides assurance that a letter has been written by a specific person, a digital signature confirms the

[13]A PKI is a system of hardware, software, policies, and people that can provide a set of information assurances (identification and authentication, confidentiality, data integrity, and nonrepudiation) that are important in conducting electronic transactions. For more information on PKI, see U.S. General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001).

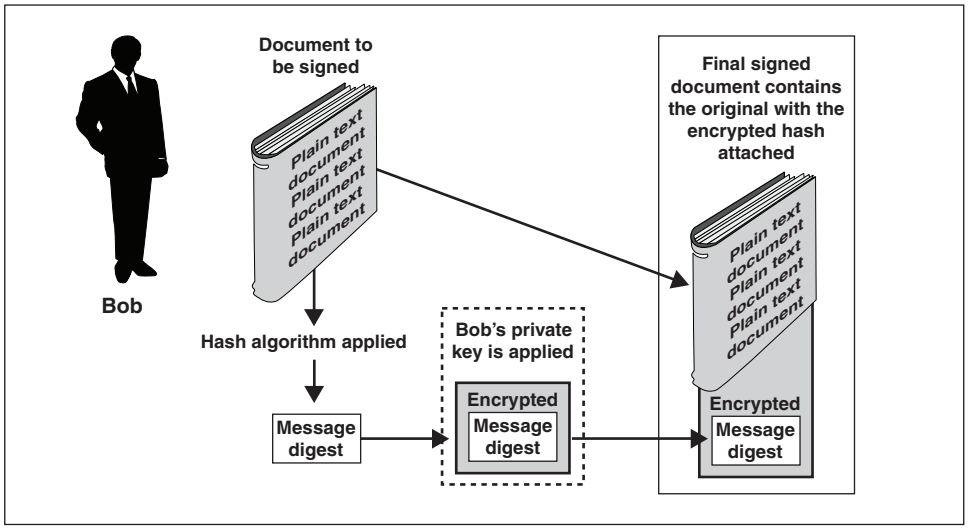
identity of a message's sender. Digital signatures are often used in conjunction with a digital certificate. A digital certificate is an electronic credential that guarantees the association between a public key and a specific entity. The most common use of digital certificates is to verify that a user sending a message is who he or she claims to be and to provide the receiver with a means to encode a reply. Certificates can be issued to computer equipment and processes as well as to individuals. For example, companies that do business over the Internet can obtain digital certificates for their computer servers. These certificates are used to authenticate the servers to potential customers, who can then rely on the servers to support the secure exchange of encrypted information, such as passwords and credit card numbers.

How the technology works

The creation of a digital signature can be divided into a two-step process based on public key cryptography, as illustrated in figure 19. As previously noted, for performance reasons, public key cryptography is not used to encrypt large amounts of data. Therefore, the first step involves reducing the amount of data that need to be encrypted. This is typically accomplished by using a cryptographic hash algorithm, which condenses the data into a *message digest*.[14] Then the message digest is encrypted, using the sender's private signing key to create a digital signature. Because the message digest will be different for each signature, each signature will also be unique; if a good hash algorithm is used, it is computationally infeasible to find another message that will generate the same message digest.

[14]A hash algorithm compresses the bits of a message to a fixed size. Because any change in the message or the algorithm results in a different value, it is not possible to reverse this process and arrive at the original information.

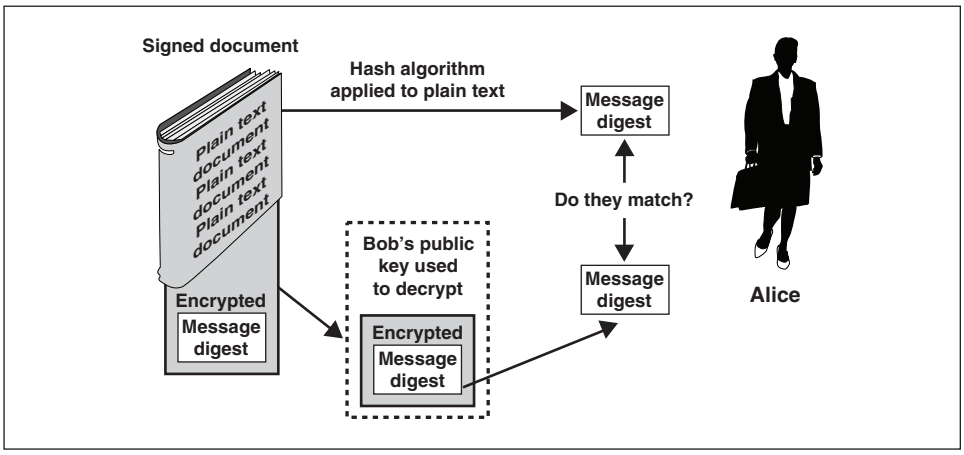
Figure 19: Creating a Digital Signature



Source: National Institute of Standards Technology and Corel Galley.

For example, if Bob wishes to digitally sign an electronic document, he can use his private key to encrypt the message digest of the document. His public key is freely available, so anyone with access to his public key can decrypt the document. Although this seems backward because anyone can read what is encrypted, the fact that Bob's private key is held only by Bob provides the proof that Bob's digital signature is valid.

Figure 20: Verifying a Digital Signature



Source: National Institute of Standards Technology and Corel Galley.

Alice (or anyone else wishing to verify the document) can compute the message digest of the document and decrypt the signature using Bob's public key (see figure 20). Assuming that the message digests match, Alice then has three kinds of security assurance. First, the digital signature ensures that Bob actually signed the document (authentication). Second, it ensures that Bob in fact sent the message (nonrepudiation). And third, because the message digest would have changed if anything in the message had been modified, Alice knows that no one tampered with the contents of the document after Bob signed it (data integrity). Of course, this assumes that (1) Bob has sole control over his private signing key and (2) Alice is sure that the public key she used to validate Bob's messages really belongs to Bob.

Digital certificates address this need to link an individual to his or her public key. A digital certificate is created by placing the individual's name, the individual's public key, and certain other identifying information in a small electronic document that is stored in a directory or other database. Directories may be publicly available repositories kept on servers that act like telephone books in which users can look up others' public keys. The digital certificate itself is created by a trusted third party called a certification authority, which digitally signs the certificate, thus providing assurance that the public key contained in the certificate does indeed belong to the individual named in the certificate. Certification authorities are a main component of a PKI, which uses cryptographic techniques to generate and manage digital certificates.

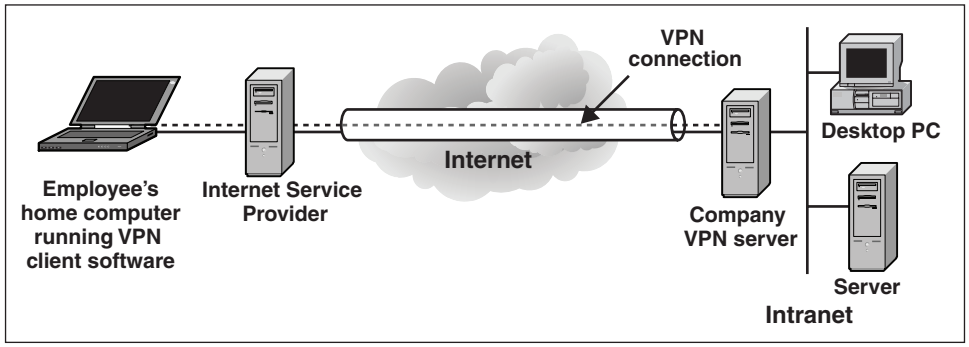
Effectiveness of the technology

Within an organization, separate key pairs are necessary to support both encryption and digital signatures, and a user's private encryption key should normally be copied to a safe backup location. This provides the organization with the ability to access encrypted data if the user's original private encryption key becomes inaccessible. For example, the organization would have an interest in decrypting data should the private key be destroyed or lost or if the user were fired, incapacitated, or deceased. However, copies of the private keys used for digital signatures should never be made, because they could fall into the wrong hands and be used to forge the owner's signatures.

By linking an individual to his or her public key, digital certificates help to provide assurance that digital signatures are used effectively. However, digital certificates are only as secure as the public key infrastructure that they are based on. For example, if an unauthorized user is able to obtain a private key, the digital certificate could then be compromised. In addition, users of certificates are dependent on certification authorities to verify the digital certificates. If a valid certification authority is not used, or a certification authority makes a mistake or is the victim of a cyber attack, a digital certificate may be ineffective.

Virtual Private Networks

Figure 21: Illustration of a Typical VPN



Source: GAO analysis and Microsoft Visio.

What the technology does

A VPN is a private network that is maintained across a shared or public network, such as the Internet, by means of specialized security procedures. VPNs allow organizations or individuals to connect a network between two or more physical locations (for example, field offices to organization headquarters) without incurring the costs of purchasing or

leasing dedicated telephone lines or frame relay circuits[15] (see figure 21). Through measures like authentication and data encryption, cryptographic VPNs can establish a secure virtual connection between physical locations.

VPNs can be implemented through hardware, existing firewalls, and standalone software applications. To a user, VPNs appear no different than traditional networks and can be used normally whether the user is dialing in from home or accessing a field office from headquarters. VPNs are typically used in intranets and extranets and in remote access connections.

- Intranets are interlinked private networks within an enterprise that allow information and computer resources to be shared throughout an organization. Some organizations have sensitive data on a LAN that is physically disconnected from the rest of the organization's intranet. This lack of connectivity may cause data on the LAN to be inaccessible to users. A VPN can be used to allow the sensitive LAN to be physically connected to the intranet, but separated by a VPN server. Only authorized users would be able to establish a VPN connection with the server to gain access to the sensitive LAN, and all communications across the VPN could be encrypted for data confidentiality.

- Remote access VPNs simplify the process of remote access, allowing off-site users to connect, via the Internet, to a VPN server at the organization’s headquarters. Digital subscriber line or cable modem services allow remote VPN users to access the organization’s network at speeds comparable to those attained with on-site access.

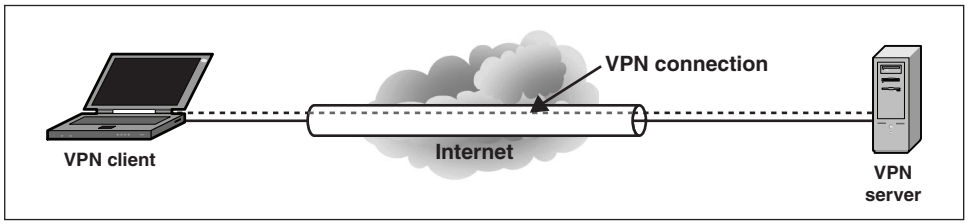
How the technology works

A VPN works by using shared public networks while maintaining privacy through security procedures and protocols that encrypt communications between two end points. To provide an additional level of security, a VPN can encrypt not only the data, but also the originating and receiving network addresses. There are two main VPN technologies, which differ in their methods of encrypting data for secure transmission over Internet connections. The first method is based on “tunneling” protocols that encrypt packets at the sending end and decrypt them at the receiving end. This process is commonly referred to as *encapsulation*, because the original, unsecured packet is placed within another packet that has been secured by encryption. The encapsulated packets are then sent through a

[15]Frame relay is a packet-switching protocol for connecting devices on a WAN.

"tunnel" that cannot be traveled by data that have not been properly encrypted. Figure 22 is a depiction of tunneling.

Figure 22: Tunneling Establishes a Virtual Connection



Source: GAO analysis and Microsoft Visio.

A commonly used tunneling protocol is IPSec.[16] IPSec VPNs connect hosts to entire private networks, encrypt IP packets, and ensure that the packets are not deleted, added to, or tampered with during transmission. Because they are based on the IP protocol, IPSec VPNs can secure any IP traffic and can be configured to support any IP-based application.

In addition to using tunneling protocols, VPNs can also use the SSL protocol, which uses a limited form of public key cryptography. SSL VPNs connect users to services and applications inside private networks , but they secure only the applications' services or data. SSL is a feature of commonly available commercial Web browsers (such as Microsoft's Internet Explorer and America Online's Netscape Navigator), and SSL VPNs use standard browsers instead of the specialized client software that is required by IPSec VPNs.

Effectiveness of the technology

VPNs can be a cost-effective way to secure transmitted data across public networks. However, the cost of implementing IPSec VPNs includes the installation and configuration of specialized software that is required on every client computer. SSL VPNs use standard Web browsers, eliminating

[16]Other tunneling protocols include Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP).

the need for client administration, but the SSL protocol often requires that applications be customized.

In addition, VPNs are only as secure as the computers that are connected to them. Because of the interconnected environment, any unsecured client computer could be used to launch an attack on the network. In particular, VPNs may be susceptible to man-in-the-middle attacks, message replay attacks, and denial-of-service attacks.[17]

Audit and Monitoring

Audit and monitoring technologies can help security administrators to routinely assess computer security, perform investigations during and after an attack, and even recognize an ongoing attack.

We describe four types of audit and monitoring technologies: intrusion detection systems, intrusion prevention systems, security event correlation tools, and computer forensics. Intrusion detection and intrusion prevention systems monitor and analyze events occurring on a system or network and either alert appropriate personnel or prevent an attack from proceeding. Audit logs are produced by many operating systems and software applications. Depending on the configuration of the logging functions, critical activities—such as access to administrator functions—are logged and can be monitored for anomalous activity. Security event correlation tools can help to detect security events and examine logs to determine the method of entry that was used by an attacker and to ascertain the extent of damage that was caused by the attack. Because of the volume of data collected on some systems and networks, these tools can help to consolidate the logs and to identify key information using correlation analysis. Computer forensics involves the identification, preservation, extraction, and documentation of computer-based evidence. Computer forensics tools are used during the investigation of a computer crime to identify the perpetrator and the methods used to conduct the attack.

[17]A *man-in-the-middle attack* is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his or her own public key for the requested one, so that the two original parties still appear to be communicating with each other directly. A *message replay attack* is one in which an attacker eavesdrops, obtains a copy of an encrypted message, and then re-uses the message at a later time in an attempt to trick the cryptographic protocol. A *denial-of-service* attack is one in which an attack from a single source overwhelms a target computer with messages, denying access to legitimate users without actually having to compromise the targeted computer.

Intrusion Detection Systems

What the technology does

An intrusion detection system (IDS) detects inappropriate, incorrect, or anomalous activity that is aimed at disrupting the confidentiality, availability, or integrity of a protected network and its computer systems. An IDS collects information on a network, analyzes the information on the basis of a preconfigured rule set, and then responds to the analysis.

A special type of IDS, known as a honeypot, acts as a decoy server or system that gathers information about an attacker or intruder—such as the method of intrusion and the vulnerabilities exploited—in order to improve security methods. To attract attackers, honeypots appear to contain important data, but instead contain false information. A honeypot can be set up to alert a system administrator of an attack via e-mail or pager, allowing the administrator to ensure that the honeypot is not used as a springboard for future attacks.

How the technology works

There are three common types of IDS, classified by the source of information they use to detect intrusion: network-based, host-based, and application-based.

Network-based IDSs detect attacks by capturing and analyzing network packets. When placed in a network segment, one network-based IDS can monitor the network traffic that affects multiple hosts that are connected to that network segment. Network-based IDSs often consist of a set of single-purpose sensors or hosts, placed at various points in a network. These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console. Because these sensors are limited to running the IDS application only, they can more easily be secured against attacks. Many of these sensors are designed to run in “stealth” mode, making it more difficult for an attacker to detect their presence and location.

Host-based IDSs collect information from within an individual computer system and use that information to detect intrusions. Host-based IDSs can determine exactly which processes and user accounts are involved in a particular attack on the system. Furthermore, unlike network-based IDSs, host-based IDSs can more readily “see” the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes that are usually targeted by attacks. Host-based IDSs normally use two types of information sources: operating system

audit trails and system logs. Operating system audit trails are usually generated at the innermost level of the operating system; therefore these trails are more detailed and better protected than system logs. Some host-based IDSs are designed to support a centralized IDS management and reporting infrastructure that can allow a single management console to track many hosts. Others generate messages in formats that are compatible with a network management system.

Application-based IDSs are a special subset of host-based IDSs that analyze the events occurring within a specific software application. The most common information sources used by application-based IDSs are the application's transaction log files. Because they directly interface with the application and use application-specific knowledge, application-based IDSs can detect the actions of authorized users who are attempting to exceed their authorization. This is because such problems are more likely to appear in the interaction among the user, the data, and the application.

These IDSs are characterized by four primary qualities: source of information, method of analysis, timing, and response.

IDSs have two primary methods of performing analysis. Signature-based (sometimes referred to as knowledge-based, or pattern-based) analysis relies on previous known attacks to detect an attack that is occurring. The IDS analyzes system activity, looking for events that match a predefined pattern of events that describes known attacks. If the analysis of data reveals that an attack is ongoing or a vulnerability is being exploited, an alarm is generated. Anomaly-based (also referred to as behavior-based) analysis compares the current operation of a system or network against a valid or accepted system behavior. An anomaly-based IDS creates a baseline of normal (valid or accepted) behavior through various collection methods. If the current behavior of the system is not within the normal boundaries of behavior, then it would be interpreted by the IDS as an attack.

IDSs can use either an interval-based or real-time timing method. The interval-based timing method analyzes the data on a predetermined schedule. This method allows an IDS to collect a large amount of data. The real-time method analyzes and responds to the data as they come in, allowing administrators to respond in real time to attacks.

IDSs can respond to possible attacks using either an active or a passive response strategy. An active response IDS is referred to as an intrusion prevention system (IPS). A passive-response IDS will typically generate an

alarm for an administrator. The alarm may appear on the administrator's screen and provide the administrator with information such as the type of attack, the location of the attack, the threat level, how it should be responded to, and possibly whether the attack is successful. A passive response IDS relies on a human to take action in response to the alert.

Effectiveness of the technology

IDSs cannot instantaneously detect, report, or respond to an attack when there is a heavy network or processing load. Therefore, IDSs are vulnerable to denial-of-service attacks; a malicious individual could send large amounts of information through a network to overwhelm the IDS, allowing the individual to launch another attack that would then go unnoticed by the IDS. IDSs rely on available attack information, and they are not as effective when protecting against unknown attacks, newly published attacks, or variants of existing attacks. In addition, IDSs are not always able to automatically investigate attacks without human involvement.

The effectiveness of an IDS can be somewhat determined by the number of false positives and false negatives that it generates. A false positive occurs when the IDS alerts that there is an attack occurring, when in fact there is no attack. A false negative occurs when the IDS fails to alert that an attack is occurring. Overall, with anomaly-based IDSs, false positives are numerous because of the unpredictable behaviors of users and networks. Administrators must devote a fair amount of time to regularly reviewing the IDS logs and to fine-tuning the IDS to limit the number of false alarms. If excessive false alarms occur, future alarms are increasingly likely to be ignored. Sometimes the IDS may be disabled for the sake of convenience. An attacker could exploit this vulnerability by slowly changing the accepted operation of the system or network recognized by the IDS, allowing for a larger attack to occur at a future time. The attacker could accomplish this by affecting the baseline as it is being created or by later slowly attacking the system so that the baseline moves to a new threshold of accepted behavior. Also, if an anomaly-based IDS is used while an attack is occurring, the normal behavior accepted by the IDS will include behaviors that are characteristic of an attack. Anomaly-based IDSs also take a varying amount of time to compute the valid or accepted behavior, so that for a period of time the IDS will not be an effective method of detecting attacks.

Intrusion Prevention Systems

What the technology does

As we have described, intrusion prevention systems (IPSs) are IDSs with an active response strategy. This means that IPSs not only can detect an intrusive activity, they also can attempt to stop the activity—ideally before it reaches its targets. Intrusion prevention is much more valuable than intrusion detection, because intrusion detection simply observes events without making any effort to stop them. IPSs often combine the best of firewall, intrusion detection, antivirus, and vulnerability assessment technologies. Their focus, however, is on the prevention of detected attacks that might exploit an existing vulnerability in the protected network or host system.

How the technology works

Like IDSs, IPSs are either network-based or host-based. They perform IDS functions and when they detect an intrusion, take action such as blocking the network traffic to prevent the attack from progressing. Network-based IPSs may simply monitor the network traffic or they may actually be "in line", which means that activity must pass through them. For example, an IPS that includes a network-based IDS that is integrated with a firewall and a host-based IDS that integrates the detection and prevention functionalities into the kernel of the operating system. Network-based IPSs thoroughly inspect data traffic, typically using specialized hardware to compensate for the processing overhead that inspection consumes.

IPSs actively respond to possible attacks by collecting additional information, changing the current environment, and taking action against the intruder. One of their common responses is to adjust firewall rules to block the offending network traffic. If an IPS responds to an attack by taking action against the intruder (commonly referred to as attack-back or strike-back), it may initiate a launch of attacks against the attacker. In another aggressive response, called "trace back," the IPS attempts to find the source of the attack.

Effectiveness of the technology

Intrusion prevention systems are the logical evolution of intrusion detection systems. Instead of dealing with the constant warning alarms of IDSs, IPSs can prevent attacks by blocking suspicious network traffic. A key value of some IPSs is their ability to "learn" what constitutes acceptable behavior and to halt activity that is not based on rules that were generated during the learning, or profiling, stage.

Network-based IPSs offer in-line monitoring of data streams throughout the network and provide the capability to prevent intrusion attempts.

Host-based IPSs allow systems and applications to be configured individually, preventing attacks against the operating system or applications. These IPSs are suitable measures to help guard unpatched and exploitable systems against attacks, but they require substantial user administration.

Unfortunately, IPSs are susceptible to errors in detecting intrusions. If the detection of incidents is not accurate, then an IPS may block legitimate activities that are incorrectly classified as malicious. Any organization that wants to utilize intrusion prevention should pay particular attention to detection accuracy when selecting a product.

Users of IPSs also face the challenge of maintaining a database of recent attack signatures so that systems can be guarded against recent attack strategies. Furthermore, IPSs cause bottlenecks in network traffic, reducing throughput across the network.

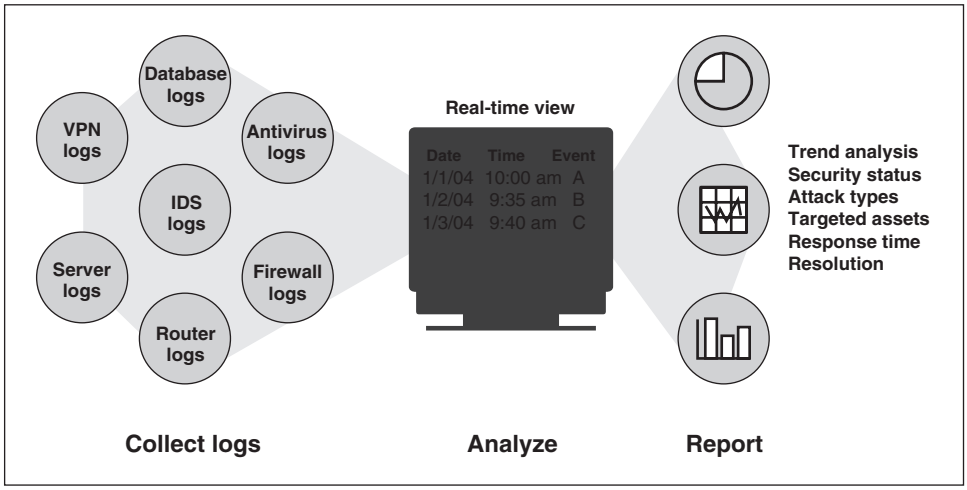
Security Event Correlation Tools

What the technology does

Security event correlation tools collect logs, or lists of actions that have occurred, from operating systems, firewalls, applications, IDSs and other network devices. Then the correlation tools analyze the logs in real time, discern whether an attack has occurred, and respond to a security incident.

Review and analysis of logs can provide a dynamic picture of ongoing system activities that can be used to verify that the system is operating according to the organization's policies. Analyzing a single device's logs is insufficient to gain a full understand of all system activity, but the size, number, and difficulty of reading through every tool's log files is a daunting task for an administrator. Security event correlation tools address the need for an administrator to investigate an attack in a real-time setting, through analysis and correlation of all the different IDS, firewall, and server logs. Automated audit tools provide a means to significantly reduce the required review time, and they will print reports (predefined and customized) that summarize the log contents from a set of specific activities (see figure 23).

Figure 23: Typical Operation of Security Event Correlation Tools



Source: GAO and Corel Draw.

How the technology works

Security event correlation tools first consolidate the log files from various sources, such as operating systems, firewalls, applications, IDSs, antivirus programs, servers, and virtual private networks. Often, the logs from the various sources come in a variety of proprietary formats that make comparisons difficult. As part of the consolidation process, security event correlation tools normalize the logs into a standard format—for example, Extensible Markup Language (commonly referred to as XML).[18] After the normalization process, unnecessary data can be eliminated in order to decrease the chance of errors.

The normalized logs are then compared (or correlated) to determine whether attacks have occurred. A variety of correlation methods can be used, including sophisticated pattern-based analysis, which can identify similar activity on various logs that have originated from an attack. For example, an IDS might not raise a flag if a single port was being scanned. However, if that port was being scanned on multiple systems, that activity might indicate an attack. By consolidating the logs from the various IDSs, correlation tools may detect this type of attack. A second method of

[18]XML is a flexible, nonproprietary set of standards for tagging information so that it can be transmitted over a network such as the Internet and readily interpreted by disparate computer systems.

analysis is called anomaly detection. In this method, a baseline of normal user activity is taken, and logged activities are compared against this baseline. Abnormal activity can then be interpreted as potentially indicating an attack. Another correlation method considers the significance of the logged event, which can be calculated as the probability that the attack would have succeeded.

If an attack is detected, the tools can then respond either passively or actively. A passive response means that no action is taken by the tool to stop the threat directly. For example, notifications can be sent to system administrators via pagers or e-mail, incidents can be logged, and IP addresses can be added to intruder or asset watch lists. An active response is an automated action taken by the tool to mitigate the risk. For example, one active response is to block the attack through interfaces with firewalls or routers.

Effectiveness of the technology

Correlation tools are limited in their ability to interface with numerous security products; they may not be able to collect and correlate logs from certain products. In addition, these tools rely on the sufficiency and accuracy of the logs, and they cannot detect attacks that have bypassed the various security devices such as the firewall and IDS. If an attacker were able to compromise the logs, then the security event correlation tool could be analyzing false information. Encryption and authentication to ensure the security and integrity of the data may mitigate this risk.

Computer Forensics Tools

What the technology does

Computer forensics tools are used to identify, preserve, extract, and document computer-based evidence. They can identify passwords, logons, and other information in files that have been deleted, encrypted, or damaged. During the investigation of a computer crime, these tools are used to determine the perpetrator and the methods used to conduct the attack.

There are two main categories of computer forensics tools: (1) evidence preservation and collection tools, which prevent the accidental or deliberate modification of computer-related evidence and create a logical or physical copy of the original evidence, and (2) recovery and analysis tools, which provide data recovery and discovery functions. A few commercially available computer forensic products incorporate features of both categories and claim to provide a complete suite of forensic tools.

How the technology works

Evidence Preservation and Collection Tools

Write protection and disk imaging software are used to preserve and copy computer evidence while preserving its integrity.

There are several techniques that are used by write protection software, which prevent or disable a user's attempts to modify data (or perform the "write" operation) on a computer's hard drive or other computer media. In one method, the write protection software attempts to gain exclusive access to the media through mechanisms specific to the operating system. If exclusive access can be gained, all other software applications will be prevented from accessing and modifying the locked media. Another method utilizes a separate software component that is installed as part of the operating system and is loaded when the operating system starts (and before any other application can execute).

Disk imaging is a process that attempts to copy every bit of data from one physical computer medium to another, similar medium. This type of duplication is known as a physical disk copy, and it involves copying all data, including files, file names, and data that are not associated with a file. Disk imaging tools may also perform varying degrees of integrity checking to verify that all data have been copied without error or alteration. The most common technique used to verify data integrity is a digital signature or a checksum algorithm.

Analysis Tools

These tools can recover deleted files by taking advantage of a common technique that is typically employed by commercial operating systems. When a user deletes a file from a computer medium (such as a floppy disk or hard drive), many operating systems do not destroy the data contained in the files. Instead, the space occupied by the deleted file is marked as available, or unallocated, so it can be reused as new files are created. The unallocated data contained in those deleted files may still remain on the medium. Analysis tools that recover unallocated data examine a specific structure and organization of information (called a file system) as it is stored on computer media. Because common operating systems maintain data in unique file systems that vary greatly, these analysis tools are typically designed for a specific file system.

Other analysis tools examine text files to identify the occurrence and frequency of specific words or patterns. They can generate a word index by creating a database of every word or delimited string that is contained

within a single file, a collection of files, or an entire medium. They can also search multiple files or entire media for the occurrence of specified strings or words, as well as performing advanced searches using Boolean expressions.[19] Some tools have the capability to perform fuzzy logic searches, which search for derivatives of a word, related words, and misspelled words. For example, when searching for files containing the word "bomb", files that contain "bombed", "explosive", or "bommb" may also be considered as matches.

Other analysis tools identify files by their type or individual identity, a method that can reduce the volume of data that an investigator must analyze. File type identification is based on a file signature—a unique sequence of values stored within a file that may be as short as 2 characters or longer than 12 characters. The longer the sequence, the greater the uniqueness of the signature and the less likely it is a file that will be mislabeled. Individual file identification is also signature-based, but the method calculates a signature over an entire file or data unit. One approach utilizes a representation that is both efficient in storage requirements and reliable in terms of its uniqueness, such as hashing algorithms.

Effectiveness of the technology

There are many different automated tools that are routinely used by law enforcement organizations to assist in the investigation of crimes involving computers. These tools are employed to generate critical evidence that is used in criminal cases. However, there are no standards or recognized tests by which to judge the validity of the results produced by these tools. Computer forensic tools must meet the same standards that are applied to all forensic sciences, including formal testable theories, peer-reviewed methodologies and tools, and replicable empirical research. Failing to apply standards may result in contaminating or losing critical evidence. It is important to obtain legal advice and consult with law enforcement officials before undertaking any forensic activities in situations where criminal or civil investigation or litigation is a potential outcome.

[19]In Boolean searches, an "and" operator between two words or other values (for example, "pear AND apple") means one is searching for documents containing both of the words or values, not just one of them. An "or" operator between two words or other values (for example, "pear OR apple") means one is searching for documents containing either of the words.

Configuration Management and Assurance

Configuration management and assurance technologies help security administrators to view and change the security settings on their hosts and networks, verify the correctness of the security settings, and maintain operations in a secure fashion under duress. Technologies that assist configuration management and assurance include policy enforcement tools, network management, continuity of operations tools, scanners for testing and auditing security, and patch management.

Policy enforcement tools help administrators define and ensure compliance with a set of security rules and configurations, such as a password policy, access to systems and files, and desktop and server configurations. Management and administration tools are used to maintain networks and systems. These tools incorporate functions that facilitate central monitoring of the security posture of networks and systems. Network management tools obtain status data from network components, make configuration changes, and alert network managers of problems.

To provide continuity of operations, there are secure backup tools that can restore system functionality and data in the event of a disruption. These products are used to account for naturally occurring problems, such as power outages, and are now also being applied to help address problems resulting from malicious cyber attacks. Tools are also available to help systems and networks to continue to perform during an ongoing attack.

Scanners are common testing and audit tools that are used to identify vulnerabilities in networks and systems. As part of proactive security testing, scanners are available that can be used to probe modems, Internet ports, databases, wireless access points, and Web pages and applications. These tools often incorporate the capability to monitor the security posture of the networks and systems by testing and auditing their security configurations.

Patch management tools help system administrators with the process of acquiring, testing, and applying fixes to operating systems and applications. Software vendors typically provide these fixes to correct known vulnerabilities in their software.

Policy Enforcement Applications

What the technology does

Policy enforcement technologies allow system administrators to perform centralized monitoring of compliance with an organization's security policies.[20] These tools examine desktop and server configurations that define authorized access to specified devices and compare these settings against a baseline policy. They typically provide multilevel reports on computer configurations, and some products have the capability to fix various identified problems. They also provide a centralized way for administrators to use other security technologies, such as access control and security event and correlation tools.

How the technology works

Policy enforcement tools generally have four main functions:

Policy definition. These tools have the functionality to help establish baseline policy settings. Policies can include features like minimum password requirements and user and group rights to specific applications. Some products include policy templates that can be customized and distributed to users for review and signatures.

Compliance checking. After a security policy has been defined, these tools can compare current system configurations with the baseline settings. Compliance can be monitored across multiple administrative domains and operating systems from a central management console. For example, compliance checking could include testing for a particular setting in multiple systems' configuration files, checking the audit configuration on a subset of computers, or checking that console passwords fit the policies of the organization (for example, using the correct length of characters in a password, using alphanumeric characters, and periodically changing passwords). The tools often allow customized checks to be defined.

Reporting. Basic reporting templates are generally included with these tools, such as templates for configurations, user accounts, access controls, and software patch levels. In addition, users can customize reports and create ad hoc queries for specific information on particular computers.

[20]Policy is defined as a set of configurations and access controls that affect the overall security stance of a user, group, device, or application.

These reports can consolidate information, such as which users have not recently logged on to a system and which computers are running unpatched applications. The reports can be tailored differently for security personnel and management.

Remediation. Some policy enforcement tools allow problems that have been discovered to be proactively fixed. For example, if the latest security software patch has not been installed for a particular application, some tools automatically download patches from a vendor's Web site and either alert an administrator or install the patches directly onto the system.

Effectiveness of the technology

Policy enforcement software can provide for centralized monitoring, control, and enforcement. However, the software's effectiveness is largely governed by the security policies of the organization. These tools can only assist in monitoring and enforcing those policies that organizations choose to implement. As such, they can be only as good as the policies that the organization defines. In addition, some policy enforcement tools do not work on all operating systems, and installation and configuration can be arduous.

Network Management

What the technology does

Network management is the ability to control and monitor a computer network from a central location. Network management systems consist of software programs and dedicated computer hardware that view the entire network as a unified architecture in order to obtain status data from network components, make configuration changes, and alert network managers to problems. The International Organization for Standardization defines a conceptual model for describing the five key functional areas of network management (and the main functions of network management systems):

- **Fault management** identifies problems in nodes, the network, and the network's operation to determine their causes and to take remedial action.
- **Configuration management** monitors network configuration information so that the effects of specific hardware and software can be managed and tracked.
- **Accounting management** measures network utilization of individual users or groups to provide billing information, regulate users or groups, and help keep network performance at an acceptable level.

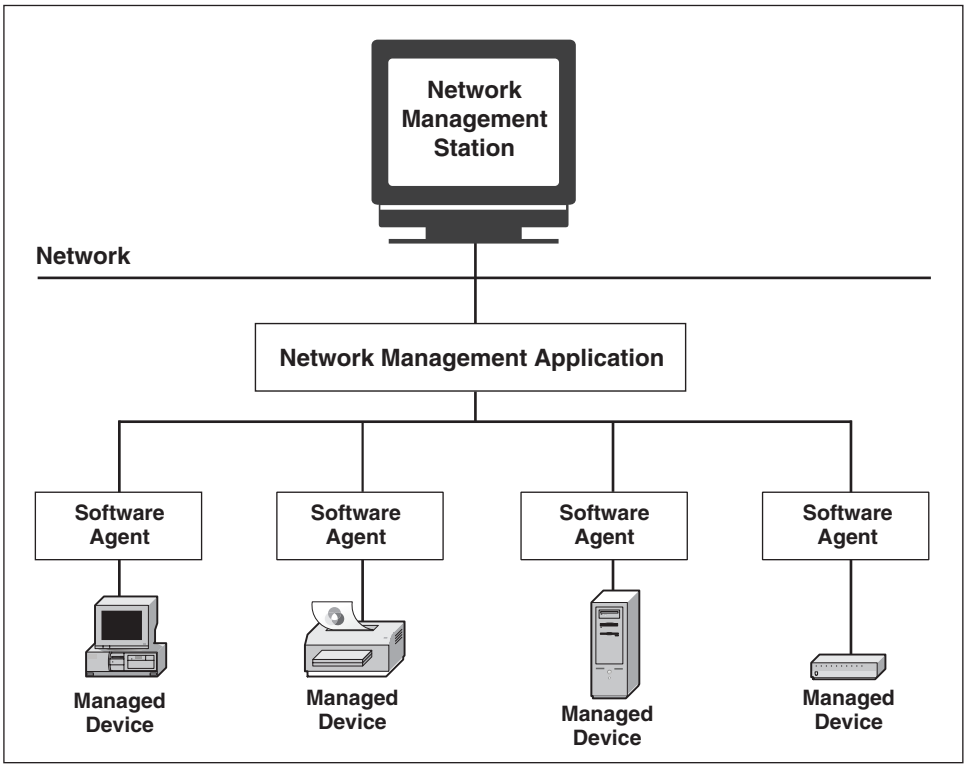
- **Performance management** measures various aspects of network performance, including gathering and analyzing statistical system data so that performance may be maintained at an acceptable level.

- **Security management** controls access to network resources by limiting access to network resources and providing notification of security breaches and attempts, so that information cannot be obtained without authorization.

How the technology works

A network management system typically consists of managed devices (the network hosts); software agents, which communicate information about the managed devices; a network management application, which gathers and processes information from agents; and a network management station, which allows an operator to view a graphical representation of the network, control managed devices on the network, and program the network management application. Figure 24 is an example of a typical network management architecture.

Figure 24: Typical Network Management Architecture



Sources: Corel Draw and Microsoft Visio.

The network management station receives and processes events from network elements and acts as the main console for network operations. The network management station displays a graphical network map that highlights the operational states of critical network devices such as routers and switches. Each network device is represented by a graphical element on the management station's console, and different colors are used to represent the current operational status of network devices, based on status notifications sent by the devices. These notifications (usually called events) are placed in a log file.

The functionality of network management software (network management applications and agents) depends on the particular network management protocol that the software is based on. Most systems use open protocols. However, some network management software is based upon vendor-specific proprietary protocols. The two most common network management protocols are the Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP). SNMP is

widely used in most LAN environments. CMIP is used in telecommunication environments, where networks tend to be large and complex.

Effectiveness of the technology

Network management systems can be quite expensive and they are often complex. The complexity is primarily in the network management protocols and data structures that are associated with the network management information. Also, these systems require personnel with the specialized training to effectively configure, maintain and operate the network management system.

Many network management systems cannot support network devices that use vendor-specific protocols.

Continuity of Operations Tools

What the technology does

Continuity of operations tools provide a complete backup infrastructure to keep the enterprise's data resources online and available at multiple locations in case of an emergency or planned maintenance, such as system or software upgrading. They maintain operational continuity of the storage devices and host and database levels. Continuity-of-operations tools include *high-availability systems*, which link two or more computers together to provide continuous access to data through systems redundancy (known as clustering); *journaling file systems*, which maintain specific information about data to avoid file system errors and corruption; *load-balancing* technology, which distributes traffic efficiently among network servers so that no individual server is overburdened; and *Redundant Array of Independent Disk (RAID)* technology, which allows two or more hard drives to work in concert for increased fault tolerance[21] and performance.

How the technology works

High-availability systems use *clustering*, which refers to two or more servers set up in such a way that if an application running on one server fails then it can be automatically restarted or recovered on another server. This is referred to as fail over from one server or node in the cluster to another. High-availability systems utilize fail over operations to automatically switch to a standby database, server, or network if the

[21]Fault tolerance is the ability of a system to respond gracefully to an unexpected hardware or software failure.

primary system fails or is temporarily shut down for servicing. Some high-availability systems can also perform remote backups, remote mutual takeovers, concurrent access operations, and remote system recoveries. These functions are described below:

- In a *remote backup*, a remote geographic site is designated as the hot backup site that is live and ready to take over the current workload. This backup site includes hardware, system and application software, and application data and files. In the event of a failure, the failed site's application workload automatically moves to the remote hot backup site.

- In a *remote mutual takeover*, geographically separated system sites are to be designated as hot backups for each other. Should either site experience a failure, the other acts as a hot backup and automatically takes over the designated application workload of the failed site. Two different workloads running at two different sites are protected.

- In *concurrent access*, systems at both sites are concurrently updating the same database.

- In *remote system recovery*, data can be resynchronized and a failed system that has been restored to operation can be reintegrated with the remote hot backup. In a process known as file mirroring, the failed system is updated with current application data and files that were processed by the backup system after the failed system ceased operations. Upon completing restoration of an up-to-date data and file mirror, the high-availability system will resume synchronized system operations, including the mirroring of real-time data and files between the system sites. This can occur while the remote backup is in use.

A *journaling file system* ensures that the data on a disk has been restored to its pre-failure configuration. It also recovers unsaved data and stores them in their intended locations (had the computer not failed), making the journaling file system an important feature for mission-critical applications. A journaling file system transaction treats a sequence of changes as a single operation and tracks changes to file system metadata and user data. The transaction guarantees that either all or none of the file system updates are done.

For example, the process of creating a new file modifies several metadata values. Before the file system makes those changes, it creates a transaction to record the intended changes. Once the transaction has been

recorded on disk, the file system modifies the metadata and the transaction is stored on the journaling file system. In the event of a system failure, the file system is restored to a consistent state by repeating the transactions listed in the journal. Rather than examining all metadata, the file system inspects only those portions of the metadata that have recently changed.

Load-balancing technology distributes processing and communications activity evenly across a computer network by transferring the tasks from heavily loaded processors to the lightly loaded ones. Load-balancing decisions are based on three policies: an information policy, which specifies the amount of load information made available; a transfer policy, which specifies the current workload of the host and the size of the job; and a placement policy, which specifies proper allocation of processes to the different computer processors.

RAID systems provide large amounts of storage by making the data on many smalls disks readily available to file servers, host computers, or the network as a single unit (known as an *array*). The design of the array of disks is an important determinant of performance and data availability in a RAID system. In addition to the array of multiple disks, RAID systems include a controller—an intelligent electronic device that routes, buffers and manages data flow between the host computer and the network array of disks. RAID controllers can organize data on the disks in several ways in order to optimize the performance and reliability of the system for different types of applications. RAID can also be implemented in software.

Effectiveness of the technology

The continuity-of-operations technologies can help an organization increase the availability of its mission-critical applications. Some of the technologies such as RAID and journaling file system increase the ability of a single server to survive a number of failures. For many businesses, the combination of RAID, journaling file system, and redundant power supply can provide adequate protection against disruptions.

Organizations that cannot tolerate an application outage of more than a few minutes may deploy a high-availability system that uses clustering. Clustering has a proven track record as a good solution for increasing application availability. However, clustering is expensive because it requires additional hardware and clustering software, and is more complex to manage than a single system.

Scanners

What the technology does

Scanners help identify a network's or a system's security vulnerabilities. There are a variety of scanning tools, including port scanners, vulnerability scanners, and modem scanners.[22]

Port scanners are used to map networks and identify the services running on each host by detecting open TCP and UDP ports. Vulnerability scanners are used to identify vulnerabilities on computer hosts and networks and make use of the results generated by a port scanner. The tools have reporting features to list the vulnerabilities they identified and may provide instructions on how to reduce or eliminate the vulnerability. Many scanners are now equipped to automatically fix selected vulnerabilities.

Modem scanners, also known as *war dialers*, are programs that identify phone numbers that can successfully make a connection with a computer modem. Unauthorized modems provide a means to bypass most or all of the security measures in place to stop unauthorized users from accessing a network—such as firewalls and intrusion detection systems.

How the technology works

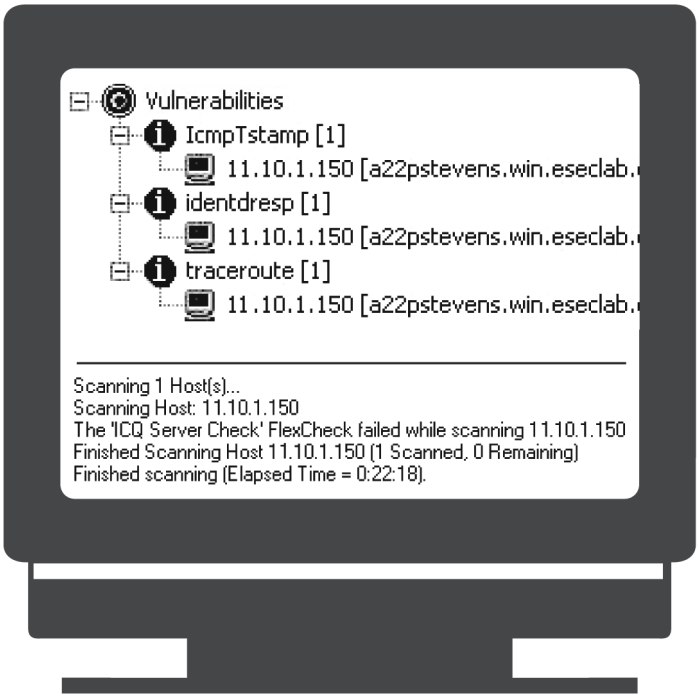
Port scanners use methods known as *ping sweeps* and *port scans* to map networks and identify services in use. Ping sweeps are considered the most basic technique for scanning a network. A ping sweep determines which range of IP addresses map to computers that are turned on by sending communication requests (known as Internet Control Message Protocol (ICMP) ECHO requests) to multiple IP addresses. If a computer at a target address is turned on, it will return a specific ICMP ECHO reply. In port scanning, the scanner sends a message to a specific port on a target computer and waits for a response. The responses to a scan can allow the scanner to determine (1) which ports are open, and (2) the operating system the computer is running (certain port scans only work on certain operating systems). The type of message sent and the information the scanner receives can distinguish the various types of port scans.

Vulnerability scanners are software applications that can be used to identify vulnerabilities on computer hosts and networks. Host-based scanners must be installed on each host to be tested, and they typically require administrative-level access to operate. Network-based scanners

[22]Other scanning tools include database scanners, Web application scanners, and wireless packet analyzers.

operate on an organization's network and identify vulnerabilities on multiple computers. Whether host-based or network-based, vulnerability scanners automatically identify a host's operating system and active applications; they then compare these with the scanner's database of known vulnerabilities. Vulnerability scanners employ large databases of known vulnerabilities to identify vulnerabilities that are associated with commonly used operating systems and applications. When a match is found, the scanner will alert the operator to a possible vulnerability. Figure 25 shows a sample screen from a vulnerability scanner.

Figure 25: Example of a Vulnerability Scanner Screen



Sources: GAO and Corel Draw.

Modem scanners are software programs that automatically dial a defined range of phone numbers and track successful connections in a database. Some modem scanners can also identify the particular operating system running on the computer, and they may be configured to attempt to gain access to the system by running through a predetermined list of common user names and passwords.

Effectiveness of the technology

Port-scanning applications have the capability to scan a large number of hosts, but they do not directly identify known vulnerabilities. However,

some vulnerability scanners can make use of a port scanner's output to target specific network hosts for vulnerability scanning. Vulnerability scanners can identify the vulnerabilities and suggest how to fix them, but they may not themselves have the capability to fix all identified vulnerabilities. They have been known to generate false positives (i.e., detecting a vulnerability that does not exist) and false negatives (i.e., not detecting a vulnerability that exists). While false positives are irrelevant warnings that can be ignored, false negatives can result in overlooking critical security vulnerabilities. Also, their effectiveness is linked to the quality of the database of known vulnerabilities; if the database is not up to date, vulnerability scanners might not identify newly discovered vulnerabilities.

Patch Management

What the technology does

Patch management tools automate the otherwise manual process of acquiring, testing, and applying patches to multiple computer systems.[23] These tools can either be stand-alone patch management products or the patch component of systems management products. Patch management tools are used to identify missing patches on each system, deploy patches to a single or multiple computers, and generate reports to track the status of a patch across a number of computers. Some tools offer customized features, including automated inventorying and immediate notification of new patches. While patch management tools primarily support the Windows operating system, they are expanding to support multiple platforms.

How the technology works

Patch management tools have various system requirements, such as specific applications, servers, and service pack levels, depending on the tool selected. Patch management tools can be either *scanner-based (non-agent)* or *agent-based*. Agent-based tools place small programs, or agents, on each computer. The agents periodically poll a patch database—a server on a network—for new updates and apply the patches pushed out by the administrator. This architecture allows for either the client or the server to initiate communications, which means that individual computers can either query the patch database or allow the server to perform a scan to

[23]A patch is an upgrade designed to fix a serious flaw (that is, a vulnerability) in a piece of software and is typically developed and distributed as a replacement for or an insertion in compiled code.

determine their configuration status. Some patch management vendors have contractual agreements with software vendors to receive pre-notification of vulnerabilities and related patches before they are publicly released. These patch management vendors test the patch before it is made available at a designated location (for example, a server), where they can be automatically downloaded for deployment. The agents will then install the patches for systems meeting the patch requirements.

Scanner-based tools scan the computers on a network according to provided criteria, such as domain or IP range, to determine their configurations. The server initiates communication with the client by logging in and querying each machine as a domain or local administrator. Patches are downloaded from the vendor's Web site and stored at a designated location to be installed to the target machine.

Most tools also have built-in knowledge repositories that compare the systems' established versions against lists that contain the latest vulnerabilities and notifications of fixes. They also have the capability to make recommendations on which patches to deploy on what machines. Additionally, these tools can analyze whether the relevant patch has been deployed to all affected systems. Many tools can also prioritize patch deployment and dependencies on each system. This capability can allow for logical groupings of target machines in order to streamline the patch installation process.

Effectiveness of the technology

While patch management tools can automate patch delivery, it is still necessary to determine if a particular patch is appropriate to apply. In addition, patches may need to be tested against the organization's specific systems configurations. The complexity of the organization's enterprise architecture determines the difficulty of this task. Also, some of these tools are not consistently accurate and will incorrectly report that a patch is missing when it was actually installed (that is, a false negative) or report that patches have been installed on unpatched systems (that is, a false positive). Furthermore, the automated distribution of patches may be a potential security exposure because patches are a potential entry point into an organization's infrastructure.

Agent-based products can reduce network traffic because the processing and analysis are offloaded to the target system and are not done on the network. In this kind of implementation, the work is performed at the client, which offloads the processing and analysis to the individual computers and saves the data until it needs to report to the central server.

Agent-based products, however, require more maintenance, deployment, and labor costs because of their distributed architecture. Additionally, the task of installing agents on each machine requires more work on the front-end. Agent-based tools are better suited for larger networks because they can typically provide a real-time network view.

Scanner-based tools are easier and faster to deploy and do not present distributive management concerns. However, they can significantly increase network traffic because tests and communications travel over the network whenever a scan is requested. Additionally, computers not connected to the network at the time scans are performed are not accounted for. As such, scanner-based tools are recommended for smaller, static networks.

Appendix IV: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 23, 2004

MEMORANDUM FOR: RICHARD HUNG
ASSISTANT DIRECTOR, CENTER FOR TECHNOLOGY AND ENGINEERING
GENERAL ACCOUNTING OFFICE

FROM: John P. Chase
Chief of Staff
Information Analysis and Infrastructure Protection Directorate
Department of Homeland Security

SUBJECT: Department of Homeland Security Response to the Draft GAO Technology Assessment (GAO-04-321) on Cybersecurity for Critical Infrastructure Protection

Thank you for the opportunity to comment on your draft report, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection (GAO-04-321)*. We concur with the purpose of the report and generally concur with its contents. We fully agree that the effective use of cybersecurity technologies is crucial to securing the nation's critical infrastructures. Your report effectively discusses many of the important issues in this area and will be of great value to those entrusted with protecting critical systems and networks.

We would like to offer some recommended changes which we believe will add value to your report. These changes, with supporting explanations, are contained in the attached spreadsheet. We recently developed this spreadsheet to facilitate our responses to GAO reports and recommendations. The empty column to the far right is available for GAO to respond to our comments if and when necessary. We hope you will find the spreadsheet makes it easier for you to process and correlate our responses.

We look forward to receiving your final report. If you or your staff have any questions or need additional information, please contact me or my GAO Liaison, John Daley, at 202-282-8381.

Attachment

www.dhs.gov

Appendix V: Comments from the National Science Foundation

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

OFFICE OF THE
DIRECTOR

April 12, 2004

Mr. Richard Hung
Assistant Director
Center for Technology and Engineering
General Accounting Office
Washington, DC 20548

Dear Mr. Hung:

Thank you very much for providing NSF with the opportunity to comment on the GAO draft report entitled *Technology Assessment: Cybersecurity for Critical Infrastructure Protection* (GAO-04-321). This is an important and timely report that provides broad coverage of current and emerging cybersecurity and infrastructure technologies. As the report documents, NSF has been actively engaged in the intertwined issues of critical infrastructure protection and computing for several years and has stimulated multi-disciplinary research and education in cybersecurity through workshops and programs such as the Information Technology Research (ITR) program, the Scholarships for Service program and the Cyber Trust emphasis area.

The cybersecurity research issues raised in the report are very real. While there is certainly a need to reinforce the technology that is already deployed, simply finding and patching holes in the existing computing fabric may not suffice. NSF advocates research and education that will effectively and efficiently lead to the development and deployment of a secure and trustworthy computing-enabled civil infrastructure. There remain significant challenges in technology deployment and use that lead to security problems. While the report emphasizes mitigating these challenges through after-the-fact application of technology, improvements may also be made through the immediate implementation of relatively simple changes in current infrastructure. This can be accomplished through the widespread deployment of architectures already recognized to be more resistant to attack.

It should also be noted that new technology discoveries are likely to lead to changes in fundamental architectural and implementation strategies for civil infrastructure. These can be expected to present both new security problems and new opportunities for deeper integration of cybersecurity into operational infrastructures. Major information technology shifts, for example, to open systems, decentralization, ad hoc networking, X-by-wire, and dynamically configured infrastructures, are likely to change the nature of cybersecurity problems and will change requirements for future civil infrastructures. For this reason too, NSF emphasizes the critical ongoing role of long range research both for developing newly robust infrastructures and for achieving security as an inherent property of these infrastructures. The preparation of a diverse national workforce equipped to create, develop, configure, operate and evaluate such systems is a similarly critical endeavor.

Finally, NSF notes that an essential component in security is the establishment of credible deterrents. In the realm of cybersecurity, this might be accomplished via strong forensics and effective use in law enforcement. Research in cyberforensics, to provide tools and training to law enforcement professionals, and to adequately fund aggressive investigations and prosecutions of malicious activity, may reduce overall threat and serve as a deterrent to would-be attackers.

Again, NSF very much appreciates the opportunity to comment on the report.

Sincerely,

Arden Bement
Acting Director

Appendix VI: GAO Contacts and Acknowledgments

GAO Contacts

Keith Rhodes (202) 512-6412; rhodesk@gao.gov.
Joel Willemssen (202) 512-6408; willemssenj@gao.gov.
Robert Dacey (202) 512-3317; daceyr@gao.gov.
Naba Barkakati (202) 512-4499; barkakatin@gao.gov.

Acknowledgments

Additional staff who made contributions to this report are Scott Borre, Lon Chin, Joanne Fiorino, Michael Gilmore, Richard Hung, Elizabeth Johnston, Christopher Kovach, Anjalique Lawrence, Stephanie Lee, Laura Nielsen, David Noone, Tracy Pierson, and Harold Podell.

We gratefully acknowledge the time and assistance of the following people who reviewed a draft of this report: Ken Birman, Cornell University; Earl Boebert, Sandia National Laboratories; Stephen Crocker, Shinkuro, Inc.; John Davis, Infosec Research Council; Lars Kjaer, World Shipping Council; Noel Matchett, Information Security Incorporated; and Dan Murray, American Transportation Research Institute. We also gratefully acknowledge the time and assistance provided by officials from the following infrastructure sectors: chemical, defense industrial base, energy, information technology, transportation, and water.

We also appreciate the contributions provided by the following organizations during our meeting on the use of cybersecurity technologies for critical infrastructure protection: American Transportation Research Institute; AT&T Labs Research; Bank of America; Carnegie Mellon University; Cornell University; Dartmouth College; Information Security Incorporated; Ivan Walks and Associates; Johns Hopkins Center for Civilian Biodefense Studies; RAND Corporation; Sandia National Laboratories; Shinkuro, Inc.; University of California at Davis; Washington State University; Wildman Harrold Allen and Dixon; and the World Shipping Council.

Bibliography

Institute for Information Infrastructure Protection. *Cyber Security Research and Development Agenda*. January, 2003.

International Organization for Standardization. *Information Technology– Code of Practice for Information Security Management*, ISO 17799, 2000.

International Organization for Standardization. *Information Technology-- Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model*, ISO 15408-1, 1999.

International Organization for Standardization. *Information Technology– Security Techniques – Evaluation Criteria for IT Security – Part 2: Security Functional Requirements*, ISO 15408-2, 1999.

International Organization for Standardization. *Information Technology-- Security Techniques – Evaluation Criteria for IT Security – Part 3: Security Assurance Requirements*, ISO 15408-3, 1999.

National Institute of Standards and Technology. *Guide to Selecting Information Technology Security Products*, NIST Special Publication 800-36. Gaithersburg, MD: October 2003.

National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems*, NIST Special Publication 800-53, Initial Public Draft. Gaithersburg, MD: October 2003.

National Institute of Standards and Technology. *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30. Gaithersburg, MD: October 2001.

National Institute of Standards and Technology. *Security Considerations in the Information System Development Life Cycle*, NIST Special Publication 800-64. Gaithersburg, MD: October 2003.

National Institute of Standards and Technology. *Security Metrics Guide for Information Technology Systems*, NIST Special Publication 800-55. Gaithersburg, MD: July 2003.

National Research Council. *Critical Information Infrastructure Protection and the Law: An Overview of Key Issues*. Washington, DC: National Academy Press, 2003.

National Research Council. *Cybersecurity of Freight Information Systems: A Scoping Study*. Washington, DC: National Academy Press, 2003.

National Research Council. *Innovation in Information Technology*. Washington, DC: National Academy Press, 2003.

National Research Council. *Trust in Cyberspace*. Washington, DC: National Academy Press, 1999.

U.S. General Accounting Office. *Combating Terrorism: Selected Challenges and Related Recommendations*. GAO-01-822. Washington, DC: September 20, 2001.

U.S. General Accounting Office. *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*. GAO-03-233. Washington, DC: February 28, 2003.

U.S. General Accounting Office. *Critical Infrastructure Protection: Challenges in Securing Control Systems*. GAO-04-140T. Washington, DC: October 1, 2003.

U.S. General Accounting Office. *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*. GAO-03-173. Washington, DC: January 30, 2003.

U.S. General Accounting Office. *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors*. GAO-04-699T. Washington, DC: April 21, 2004.

U.S. General Accounting Office. *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*. GAO-02-474. Washington, DC: July 15, 2002.

U.S. General Accounting Office. *High Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*. GAO-03-121. Washington, DC: January 2003.

U.S. General Accounting Office. *Information Security: Challenges in Using Biometrics*. GAO-03-1137T. Washington, DC: September 9, 2003.

U.S. General Accounting Office. *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures*. GAO-01-1073T. Washington, DC: August 29, 2001.

U.S. General Accounting Office. *Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities*. GAO-03-1138T. Washington, DC: September 10, 2003.

U.S. General Accounting Office. *Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*. GAO-03-564T. Washington, DC: April 8, 2003.

U.S. General Accounting Office. *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*. GAO/AIMD-98-92. Washington, DC: September 23, 1998.

U.S. General Accounting Office. *Information Security: Technologies to Secure Federal Systems*. GAO-04-467. Washington, DC: March 9, 2004.

U.S. General Accounting Office. *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*. GAO-01-751. Washington, DC: August 13, 2001.

U.S. General Accounting Office. *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*. GAO-02-24. Washington, DC: October 15, 2001.

U.S. General Accounting Office. *National Preparedness: Technologies to Secure Federal Buildings*. GAO-02-687T. Washington, DC: April 25, 2002.

U.S. General Accounting Office. *Technology Assessment: Using Biometrics for Border Security*. GAO-03-174. Washington, DC: November 15, 2002.

The White House. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC: February 2003.

The White House. *The National Strategy to Secure Cyberspace*. Washington, DC: February 2003.

The White House Office of Homeland Security. *National Strategy for Homeland Security*. Washington, DC: July 2002.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER