THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

TRUSTED ACCESS TASK FORCE
Screening, Credentialing, and Perimeter Access Controls Report

January 19, 2005

Table of Contents

EXECUTIVE SUMMARY

The United States Government recognizes that a number of infrastructures are critical to "our national identity and strategic purpose,"[1] and that any threats, whether implied or actual, against key facilities supporting recognized critical infrastructures could adversely affect national security and emergency preparedness (NS/EP) services. Designated as one of those critical infrastructures, the telecommunications sector is heavily relied on by the Government, other critical infrastructures, and the general public. Although industry and Government have made significant strides in protecting the infrastructure, vulnerabilities remain with regard to physical access to telecommunications facilities. This report addresses the Administration's concerns that the telecommunications infrastructure may be vulnerable because trusted physical access is granted to individuals requiring entrance to sites where telecommunications assets are concentrated without ensuring that the individual will not pose a threat to the facility or the telecommunications infrastructure at large.

Due to the functional nature of critical telecommunications facilities, numerous categories of individuals access the facilities daily and may be granted unescorted access to the facility for various periods of time. In addition, company employees can pose a threat to the security of a telecommunications facility. With approximately 90 percent of the telecommunications infrastructure's key assets owned by the private sector, protection efforts must account for both Government and private facilities. Government personnel and Government contractors are cleared through the standard Government clearance and screening processes; however, there is no standard process for vetting telecommunications employees, contractors, and vendors to certify that they are trusted members of the organizations they purport to represent. Instead, the telecommunications sector must rely on varied and limited investigations and screenings by private contractor firms that do not have access to Government databases with critical terrorist and criminal intelligence. Consequently, the telecommunications sector cannot fully protect the infrastructure against national security concerns.

A national standard for personnel screenings utilizing Federal databases, such as the program employed by the Transportation Security Administration (TSA), may be useful for industry in mitigating threats to national security. The TSA program accounts for traits within the airline environment that are similar to the telecommunications environment, including a large number of facilities with varying degrees of security and access requirements and a broad scope of employees, including contractors and vendors.

Industry and Government typically require a credential for personnel to signify the successful completion of a screening process as well as the designation of facilities to which personnel are allowed access. Because industry typically develops and issues such credentials for each facility separately or as an individual company, no highly secure, standard type of certificate-based picture identification (ID) card is employed industry-wide. The creation of such a card, as well as processes to change the access permissions allowed to the card and verify the integrity of the card, will further solidify the Nation's telecommunications infrastructure, as it will aid in the easy identification of trusted individuals (i.e., those who have passed the national screening). In

---

1 The White House, *The President's National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, March 2003, p. 6.

times of crisis and emergency, a standard credential will aid in perimeter control operations and promote speedy recovery efforts by identifying personnel with a valid need to be at the site.

Access control concerns for the telecommunications industry exist for the daily protection of static critical telecommunications facilities, but protection efforts must also consider access to national special security events (NSSE), such as national political conventions and Presidential inaugurations, as well as emergency incident response situations at which telecommunications providers are key players. However, collaboration between industry and Government for these events typically occurs on an ad hoc basis and at local levels. There is no single point of contact within the Government for these events, and no clear plan is in place for ongoing collaboration. If a standard process is established for coordination with industry on perimeter access issues at such events, it may prevent delays and confusion in assuring or restoring necessary communications services for NSSEs and emergency incident response situations.

The NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, direct the appropriate departments and agencies to—

- Coordinate with industry to:
  - Implement and support a standardized screening process for industry to voluntarily conduct screenings on persons who have regular and continued unescorted access to critical telecommunications facilities (e.g., switching facilities), including telecommunications employees and vendors, suppliers, and contractor staff, including:
    - » Modeling such a program after the current TSA program by including different relative background investigation levels for various facilities and personnel types;
    - » Partnering with the Department of Homeland Security (DHS), through TSA, to upon request from industry, conduct screenings for industry personnel working at critical private telecommunications facilities; and
    - » Working with the Network Reliability and Interoperability Council to develop industry best practices defining specific criteria for determining which telecommunications employees should be subject to screenings.
  - Make available a standard "tamper-proof," certificate-based picture identification technology to enable the positive identification of screened individuals at critical sites and to support both physical and logical access for such individuals to critical telecommunications facilities and the networks and information concerning them by building on the ongoing work of the General Services Administration's Federal Identity Credentialing Committee.
  - Build on the recommendations in the National Coordinating Center for Telecommunications (NCC) Information Sharing and Analysis Center (ISAC) report, *Preparing for a National Special Security Event,* to develop a national plan for controlling access at the perimeter of an NSSE or a disaster area. To facilitate the development of a national perimeter access plan to be incorporated in the *National Response Plan,* the Government should continue to support the screening program coordinated by the NCC ISAC with screenings facilitated by DHS and the United States Secret Service.

- Partner with the ISACs across infrastructures to implement screening, credentialing, and access control policies mirroring those recommended for the telecommunications infrastructure for all critical infrastructures.

TRUSTED ACCESS TASK FORCE
SCREENING, CREDENTIALING, AND PERIMETER ACCESS CONTROLS REPORT

1.0 INTRODUCTION

The United States Government defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[2] The Government further recognizes a number of infrastructures (e.g., Telecommunications, Energy, Water) as critical to "our national identity and strategic purpose,"[3] and that any threats, whether implied or actual, against key facilities supporting recognized critical infrastructures could adversely affect national security and emergency preparedness (NS/EP) services.

The Government not only recognizes the telecommunications sector as a critical component of NS/EP services, but also recognizes the potential for peril implied by the growing reliance on the availability of telecommunications resources by the Government, other critical infrastructures, and the general public. The increasing reliance on telecommunications resources is further complicated by the enormity of scale and geographic disparity of critical telecommunications assets.

Supporting the dispersed assets of the telecommunications infrastructure requires a diversified work force with a multitude of skills. In turn, a considerable portion of the work force requires physical access to telecommunications components in order to perform routine tasks, including administration and management. It is the requirement for physical access that uncovers a lingering concern—the telecommunications infrastructure is vulnerable to malicious acts because trusted physical access is granted to individuals requiring entrance to sites where telecommunications assets are concentrated. While most companies protect their key facilities and many have rigorous access controls in place (e.g. card readers), no standard process exists for vetting telecommunications employees, contractors, and vendors to verify that they are trusted members of the organizations they purport to represent. As the Nation increasingly relies on the private telecommunications infrastructure for critical NS/EP communications and operations, vulnerabilities related to access control procedures for critical sites must be addressed.

In March 2003, the President's National Security Telecommunications Advisory Committee's (NSTAC) Vulnerabilities Task Force issued its *Trusted Access to Telecommunications Facilities Report,* which provided several recommendations to the President of the United States on securing access to the Nation's critical telecommunications facilities.

During the NSTAC XXVI Meeting in April 2003, participants again raised the issue of trusted access to facilities, focusing on the need to improve background check processes to further

---

2 The White House, *The President's National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, March 2003, p. 6.

3 Ibid.

secure critical telecommunications facilities. Following the NSTAC XXVI Meeting, the NSTAC created the Trusted Access Task Force (TATF) and tasked it to work with Department of Homeland Security (DHS) representatives to address the following recommendations from the VTF's report:

Task 1

- Coordinate with industry and State and local Governments to develop guidance for:
  - Creating national standards and capabilities for national security background checks, screening, and National Crime Information Center (NCIC) reviews;
  - Defining the criteria for inclusion in background checks; and
  - Identifying who should be subject to background checks.

Task 2

- Analyze the data gathered during Task 1 and apply it to the concept of a national background check process to determine:
  - What is the process for carrying out background check investigations?
  - What is the desired end state for the background check process?
  - What activities need to be undertaken in the current process to meet the desired end state?
  - How should a national background check be deployed?

During the May 2004 NSTAC XXVII Meeting, Mr. Robert Liscouski, Assistant Secretary for Infrastructure Protection, DHS, emphasized the importance of the TATF's ongoing screening work. In addition, Mr. Liscouski commented that the Government needs short-term initiatives that could be undertaken to further increase security at numerous upcoming national special security events (NSSE), and that those short-term initiatives would be the basis for long–term perimeter access guidelines.

This report addresses the Administration's concerns that the telecommunications infrastructure may be vulnerable because trusted physical access is granted to individuals who require entrance to sites where telecommunications assets are concentrated without ensuring that the individual will not pose a threat to the facility or the telecommunications infrastructure at large. Specifically, the report addresses the issues outlined in Tasks 1 and 2 and also offers recommendations for improving perimeter access control in response to the tasking from Mr. Liscouski on behalf of DHS.

2.0 SCREENINGS

With approximately 90 percent of the telecommunications infrastructure's key assets owned by the private sector, protection efforts must account for both Government and private facilities. Although Government personnel and Government contractors are cleared through the standard Government clearance and screening processes, no standard process exists for the private sector to ensure personnel accessing critical telecommunications facilities do not pose a threat to NS/EP communications. The private sector currently requires a Government sponsor for such a screening and clearance, and in the absence of such a sponsor must rely on various private contractor firms to conduct screenings. The limited and varied investigative processes of these

firms typically include checks of State or local police records but do not include Federal intelligence databases—key for identifying threats to national security. Because industry has neither a national database with pertinent screening information nor access to Government databases with critical terrorist and criminal intelligence, it cannot gain as in-depth a picture as Government agencies can when performing screenings.

Due to the functional nature of critical telecommunications facilities, numerous categories of individuals access the facilities daily, including equipment vendors, fuel suppliers, janitorial services, security forces, and heating, air conditioning, plumbing, and electrical contractors. These individuals may be granted unescorted access to the facility for various periods of time. In addition to vendors, suppliers, and contractors, company employees can pose a threat to the security of a telecommunications facility. Legitimate employees with authorized access can have malicious intent, and this insider threat can be difficult to eliminate.

Access control requirements vary from site to site because each site's assets vary in terms of their degree of criticality and their numbers and types of personnel requiring access. Recognizing that standards for screening processes must reflect these differences, the task force explored several screening models, including the Nuclear Regulatory Commission and the Interagency Board, and has identified the DHS Transportation Security Administration's (TSA) screening program as a Government program similarly reflecting the environment and needs of the telecommunications industry. The TSA program accounts for a large number of facilities with varying degrees of security and access requirements, a broad scope of employees, including contractors, much like a program to secure national telecommunications facilities.

According to the June 2004 General Accounting Office report, *Aviation Security*, TSA divides the perimeters of airports into three different security areas: Secured/Security Identification Display Areas (SIDA), consisting of baggage loading areas, taxiing areas, and runways; Air Operations Areas (AOA) including taxiing and runway areas; and the sterile area. TSA's screening program encompasses all employees with unescorted access to secured airport areas as well as individuals who have regular escorted access to secured airport areas. In addition, most airport workers requiring access to secured and sterile areas are required to undergo a fingerprint-based criminal history records check and are compared against TSA's aviation security watch lists and TSA's "no fly" list.

To augment this process, TSA recently began conducting a supplementary two-part screening consisting of a name-based Federal Bureau of Investigation (FBI) NCIC check and a terrorist link analysis against selected terrorism databases for the approximately 100,000 airport workers who have access to sterile areas. TSA uses the NCIC database, a computerized index of documented criminal justice information, to conduct a criminal history record check that compares the individual's name against 19 nationwide criminal history lists. To meet TSA requirements, airport operators transmit applicants' fingerprints to a TSA contractor, who then forwards the fingerprints to TSA, who submits them to the FBI to be checked for criminal histories that could disqualify an applicant for airport employment.

Workers who perform duties in the SIDA are required to display identification badges and must undergo security awareness training, and AOA workers must follow security procedures similar to those in the SIDA. In the sterile area, all workers are required to display identification (ID)

badges and are also physically screened before being allowed to enter the area. TSA does not require airport workers who have been granted unescorted SIDA access to be physically screened for prohibited items when entering secured areas, such as baggage loading areas.[4]

In its December 2003 Final Report, the Network Reliability and Interoperability Council's (NRIC) Physical Security Subcommittee of the Homeland Security Focus Group recommended that,

"The Federal Government should develop and fund a process to enable employers to voluntarily conduct national background checks (e.g., NCIC) on employees with access to areas of critical communications infrastructure." Following on from the NRIC's recommendation, to mitigate ongoing personnel-based vulnerabilities at critical telecommunications facilities, the Federal Government could assist industry in providing screenings for any person having regular and continued unescorted access to private critical telecommunications facilities, including telecommunications employees and vendors, suppliers, and contractor staff, modeling the industry screening initiative after the current TSA model. The Government can ensure that private facilities meet the same security standard as public facilities by encouraging DHS, through TSA, to, upon request from industry, conduct screening investigations that are similar to those conducted for airport employees, on behalf of industry for a fee. In addition to conducting screening against criminal databases such as the NCIC, the Government could facilitate industry's need to screen employees with access to critical facilities for foreign terrorist concerns by utilizing Federal terrorist watch lists and other Government terrorist databases. The designation of DHS as a partner for industry screening investigations will facilitate industry's ability to conduct more comprehensive screenings by providing access to Government-protected criminal, intelligence, and financial databases. By designating this responsibility to a Government agency, the Government would mitigate privacy concerns and still ensure that industry can access the data needed to fully secure these critical infrastructures. The Government could also work with the NRIC to develop best practices defining specific criteria for which specific telecommunications employees and contractors should be subject to screenings.

3.0 CREDENTIALING

Industry and Government often require a credential for personnel to signify the successful completion of a screening process as well as the designation of facilities to which personnel are allowed access. Because industry typically develops and issues such credentials for each facility separately or as an individual company, no highly secure, standard type of certificate-based picture ID card is employed industry-wide. The creation of such a card, in addition to processes to change the access permissions, allowed to the card and verify the integrity of the card, will further solidify the Nation's telecommunications infrastructure because it will aid in the easy identification of trusted individuals (i.e., those who have passed the national screening). In times of crisis and emergency, a standard credential will aid in perimeter control operations and promote speedy recovery efforts by identifying personnel with a valid need to be at the site.

---

[4] See the U.S. General Accounting Office Report, GAO-04-728, *Aviation Security*, June 2004.

In its *Trusted Access to Critical Facilities* report, the VTF recommended that the President "lead the research and development and standards bodies' efforts to make available a standard 'tamper-proof,' certificate-based picture identification technology to enable the positive identification of individuals at critical sites." Currently, the Federal Government is addressing similar credentialing issues through the General Services Administration's (GSA) Federal Identity Credentialing Committee (FICC). The mission of the FICC is to make policy recommendations and develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture, including associated services (identity proofing, credential management, etc.), for the Federal Government.[5]

In its ongoing efforts, the FICC has produced a draft of the *Authentication and Identity Policy Framework for Federal Agencies*. The framework describes policies for issuing and monitoring physical and logical access credentials, as well as a standardized credentialing process that consists of both physical access to facilities and access to systems. The following is an overview of this framework[6]:

- Credentials must demonstrate reasonable protections against misrepresentation by using tamper-resistant characteristics;
- The credential should support both physical and logical access;
- The credential should be usable for identity authentication and electronic signature;
- The credential should be accepted throughout the Federal Government, by using smart card technology that incorporates both contact-less and contact technology in accordance with the Government Smart Card Interoperability Specification;
- Federal agencies will issue and manage access credentials for Federal personnel and other authorized individuals;
- Physical/logical access credentials must meet a minimum identity assurance level, which is accepted by all Federal organizations and deemed sufficient to meet generic Federal security requirements for e-government applications and access control; and
- The technology for electronic credentials that best meets the Government's needs at this time is Public Key Infrastructure (PKI) digital certificates.

The FICC has also developed a policy implementation requirements framework that establishes the common policy implementation for Federal agencies; this includes[7]:

- Identity Requirements: Agencies should issue Federal Identity Credentials in a consistent manner, using approved identity proofing standards;
- Physical Credential Requirements: Agencies should issue hardware tokens in a smart card form that is compliant with Government Smart Card Interoperability Specification (GSC-IS). Credentials should use a consistent topology to ensure government-wide use,

5 FICC website. http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=14516

6 See the FICC's *Draft Authentication and Identity Policy Framework for Federal Agencies*, April 8, 2004.

7 Ibid.

and also utilize a standard data format to ensure interoperability of electronic credentials and automated access systems; and

- Electronic Credential Requirement: Agencies should issue electronic credentials that are compliant with Federal standards and guidance.

As a means to further develop a national screening program for the telecommunications infrastructure, the Government could coordinate with industry to make available a standard "tamper-proof," certificate-based picture identification technology to enable the positive identification of screened individuals at critical sites and to support both physical and logical access for such individuals to critical telecommunications facilities and the networks and information concerning them. Industry and Government can standardize credentialing efforts industry-wide by tying those efforts to a national, standard employee screening program and building on the FICC's efforts to create a single credential that serves both physical and logical access purposes. While there may be a considerable financial investment on the part of industry to replace or amend existing programs to meet the industry standards for screening and credentialing, a cohesive, unified approach will raise the protection level for the industry as a whole.

4.0 PERIMETER ACCESS CONTROL

Access control concerns for the telecommunications industry exist for the daily protection of static critical telecommunications facilities, but protection efforts must also consider access to NSSEs, such as national political conventions and Presidential inaugurations, and emergency incident response situations. There is no standard Government policy or point of contact in place for private sector use in planning activities for any perimeter control issues. Collaboration typically occurs on an ad hoc basis by industry representatives at local facilities.

Industry-wide screening and credentialing standards can assuage perimeter control concerns at static facilities; however, NSSE situations require additional activity and collaboration due to the heightened awareness of the event and the concentration of potential targets. These events often include the additional complication of time constraints. No process is in place for announcing the official designation of an event as an NSSE, allowing industry to begin preparations with the Secret Service, responsible for planning NSSEs, immediately. Of additional concern is the possibility that an emergency situation may occur, turning an NSSE into an emergency incident response situation. Should this occur, the perimeter would change and the controlling authority would shift to the FBI; but no plan exists for coordinating industry activity with this new authority. Therefore, industry would be left with no means of accessing the area and delays would be created in restoring necessary services.

On June 18, 2004, the National Coordinating Center for Telecommunications (NCC) Telecom Information Sharing and Analysis Center (ISAC) released a report entitled *Preparing for a National Special Security Event.* The NCC Telecom ISAC report highlights numerous examples of service provider and NCC Telecom ISAC planning activities conducted in preparation for an NSSE. In addition, the report offers several key recommendations for improved industry/Government coordination for NSSEs, including:

- The announcement of an NSSE to the NCC Telecom ISAC in coordination with other parties necessary for event management;
- The involvement of the NCC Telecom ISAC in the development of any baseline requirements for an NSSE;
- The inclusion of the NCC Telecom ISAC in any plans or processes to test security and readiness prior to an NSSE;
- The recognition that the NCC serves as a focal point for the Federal Government to communicate with the telecommunications industry for NS/EP needs;
- The consideration and inclusion of the private sector, and specifically the NCC Telecom ISAC in support of the communication requirements of NSSEs;
- The identification and announcement of NSSE Points of Contact (i.e., Secret Service Special Agents, FBI Special Agents) to the NCC Telecom ISAC;
- The communication of procedures to the NCC Telecom ISAC regarding the appropriate credentialing process to permit employee access to telecommunications facilities before and during an NSSE; and
- The development and delivery of estimated resource requirements to service providers supporting an NSSE.

To better coordinate efforts for controlling access at the perimeter of an NSSE or a disaster area to be incorporated in the *Federal Response Plan*, the Government could continue its work with industry to build on the recommendations in the NCC Telecom ISAC report *Preparing for a National Special Security Event.* In addition, the Government currently supports a screening program coordinated by the NCC ISAC with screenings facilitated by the United States Secret Service through DHS IAIP. Using Federal terrorist lists/government databases, the program pre-screens a small subset of industry employees who may have access to physical sites or critical information concerning NSSEs and associated critical facilities. The purpose of the program is to develop a centralized process for effectively screening telecommunications employees over the long term. The telecommunications industry screening program may serve as the model for similar programs across all critical infrastructures needing access to NSSEs or associated critical facilities. As the program progresses and the participants capture lessons learned, the NSTAC will determine whether further TATF action is necessary on this issue.

As the telecommunications infrastructure is only one of 13 critical infrastructures as defined by the President's National Strategy for Homeland Security, the Government could partner with the ISACs representing the other critical infrastructures to implement screening, credentialing, and access control policies mirroring those recommended for the telecommunications infrastructure.

5.0 CONCLUSIONS

- Due to the nature of critical telecommunications facilities, numerous categories of individuals, including vendors, suppliers, contractors, and company employees, may be granted unescorted access to the facility for varying periods of time,

- No standard process exists for the private sector to ensure personnel accessing critical telecommunications facilities do not pose a threat to NS/EP communications.
- Because critical telecommunications sites have assets with varying degrees of criticality as well as varying numbers and types of persons requiring access, access control requirements also vary from site to site.
- The Government can ensure that critical private facilities meet the same security standard as critical public facilities by encouraging DHS, through TSA, to, upon request from industry, conduct screening investigations for industry for any person having regular and continued unescorted access to private critical telecommunications facilities, modeling the industry screening initiative after the current TSA program for the airline industry. Similar to the telecommunications environment, the airline environment includes a large number of facilities with varying degrees of security and access requirements, a broad scope of employees, and must include contractors and vendors.
- Industry typically develops and issues credentials for each facility separately or as an individual company; therefore, no highly secure, standard type of certificate-based picture ID card is currently employed industry-wide.
- The creation of a standard industry-wide credential, in addition to processes to change the access permissions, allowed to the card and verify the integrity of the card, will further solidify the Nation's telecommunications infrastructure, because it will aid in the identification of trusted individuals (i.e., those who have passed the national screening).
- The Federal Government is working to create a single credential that serves both physical and logical access purposes through the GSA's FICC. Based on this ongoing work and as a means to further develop a national screening program for the telecommunications infrastructure, the Government could coordinate with industry to make available a standard "tamper-proof," certificate-based picture identification. This identification technology will enable the positive identification of screened individuals at critical sites and support both physical and logical access for such individuals to critical telecommunications facilities and the networks and information concerning them.
- While there may be a considerable financial investment on the part of industry to replace or amend existing programs to meet the industry standards for screening and credentialing, a cohesive, unified approach will raise the protection level for the industry as a whole.
- Protection efforts must also consider access to NSSEs, such as national political conventions and Presidential inaugurations, and emergency incident response situations. NSSE situations require additional activity and collaboration due to the heightened awareness of the event, the concentration of potential targets, and possible time constraints.
- Collaboration between industry and Government to support NSSEs and emergency incident response situations typically occurs on an ad hoc basis by industry representatives at local facilities. No standard Government policy or point of contact exists for private sector use in planning activities for any perimeter control issues. In

addition, no process is in place for announcing the official designation of an event as an NSSE, allowing industry to begin preparations immediately with the lead Federal Agency responsible for planning NSSEs.

- The Federal Government could assist industry in addressing perimeter control issues and handling NSSE and emergency situations by continuing to work with industry through the ISACs to develop a standard coordination plan for such events. In addition, the Government could further efforts to better secure NSSEs by continuing to work with the NCC ISAC to support the screening program for industry employees who support NSSEs.

6.0 RECOMMENDATIONS

The NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, direct the appropriate departments and agencies to—

- Coordinate with industry to:
  - Implement and support a standardized screening process for industry to voluntarily conduct screenings on persons who have regular and continued unescorted access to critical telecommunications facilities (e.g., switching facilities), including telecommunications employees and vendors, suppliers, and contractor staff, including:
    - » Modeling such a program after the current TSA program by including different relative background investigation levels for various facilities and personnel types;
    - » Partnering with DHS, through TSA, to, upon request from industry, conduct screenings for industry personnel working at critical private telecommunications facilities; and
    - » Working with the NRIC to develop industry best practices defining specific criteria for determining which telecommunications employees should be subject to screenings.
  - Make available a standard "tamper-proof," certificate-based picture identification technology to enable the positive identification of screened individuals at critical sites and to support both physical and logical access for such individuals to critical telecommunications facilities and the networks and information concerning them by building on the ongoing work of GSA's Federal Identity Credentialing Committee.
  - Build on the recommendations in the NCC's ISAC report, *Preparing for a National Special Security Event*, to develop a national plan for controlling access at the perimeter of a national special security event or a disaster area. To facilitate the development of a national perimeter access plan to be incorporated in the *Federal Response Plan*, the Government should continue to support the screening program coordinated by the NCC ISAC with screenings facilitated by DHS and the United States Secret Service.

- Partner with the ISACs across infrastructures to implement screening, credentialing, and access control policies mirroring those recommended for the telecommunications infrastructure for all critical infrastructures.

APPENDIX A—TASK FORCE MEMBERS AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

Qwest	Mr. Jim Payne, Chair
BellSouth Corporation	Mr. David Barron, Vice Chair
AT&T Corporation	Mr. Harry Underhill
Lucent	Mr. Karl Rauscher
MCI	Ms. Joan Grewe
Microsoft Corporation	Mr. Bill Cooper
Nortel Networks	Dr. Jack Edwards
Raytheon	Mr. Frank Newell
Science Applications International Corporation	Mr. Hank Kluepfel
SBC Communications, Inc.	Ms. Rosemary Leffler
Sprint Corporation	Mr. Todd Colvin
VeriSign	Mr. Justin Somaini
Verizon Communications	Ms. Ernestine Gormsen

OTHER PARTICIPANTS

BellSouth Corporation	Mr. Mason Griffin
George Washington University	Dr. Jack Oslund
Lucent	Mr. Rick Krock
MCI	Mr. Frank Swenson
National Communications System	Mr. Don Smith
SBC Communications, Inc.	Ms. Suzy Henderson
Qwest	Mr. Gene Carmer
Qwest	Mr. Jon Lofstedt
Qwest	Mr. Tom Snee
Telcordia	Ms. Louise Tucker
Verizon Communications	Mr. Jim Bean

BRIEFERS

Department of Defense	Mr. Paul Grant
Department of Homeland Security	Mr. Keith Hughes
General Services Administration	Ms. Judith Spencer
Global Options, Inc.	Mr. Ed Shubert
Nuclear Regulatory Commission	Ms. Cheryl Stone
Transportation Security Administration	Ms. Pamela Friedmann
Transportation Security Administration	Special Agent Tim Upham

APPENDIX B—TRUSTED ACCESS TASK FORCE PILOT SCREENING PROGRAM SUMMARY

Since its creation in June 2003, the President's National Security Telecommunications Advisory Committee's Trusted Access Task Force (TATF) has been working with the Federal Government, as well as industry, to develop Presidential level policy guidance for the creation of national standards, criteria, and capabilities for national security background screenings, and National Crime Information Center reviews for trusted access to telecommunications facilities. During the May 2004 NSTAC XXVII Meeting, Mr. Robert Liscouski, Assistant Secretary for Infrastructure Protection, Department of Homeland Security (DHS), emphasized the importance of the TATF's ongoing work and commented that the Government needed to act quickly to ensure the security of numerous national special security events (NSSE) over the coming months, including the Democratic and Republican National Conventions. He asked the NSTAC to provide DHS with actionable recommendations on short-term initiatives that could be undertaken to further increase security at these upcoming events.

To this end, the TATF, with the assistance of the National Coordinating Center for Telecommunications (NCC) Information Sharing and Analysis Center (ISAC) member companies, proposed the establishment of a pilot program to pre-screen against Federal terrorist lists/government databases a small subset of industry employees who may have or need access to physical sites or critical information concerning NSSEs and associated critical facilities. The purposes of the trial were to surface obstacles and determine the feasibility of and necessary requirements to roll out such a centralized process for the telecommunications industry over the long term. The final screening program would coordinate on a national level the NSSE preparation efforts that are currently ongoing at the local level and develop a list of industry personnel pre-approved to support NSSEs. The screening program would serve as the model for similar programs across all critical infrastructures needing access to NSSEs or associated critical facilities. Participation in the trial program was voluntary at both the company and individual levels.

PROCESS

Each company participating in the pilot program would identify 3-5 persons either needing access to or having critical information concerning NSSEs or associated critical facilities and submit the full name, date of birth, place of birth, and social security number for each person to the Manager of the NCC. Acting on behalf of all participating companies, the Manager of the NCC identified the United States Secret Service (USSS) as the organization to conduct the screenings on behalf of industry. The Manager of the NCC contacted other departments, including the Infrastructure Coordination Division within DHS, however the USSS was deemed the most appropriate avenue for industry due to their role in planning NSSEs, their standing relationship with industry in screening for NSSEs at the local level, and their access to screening resources.

The USSS would conduct a screening on the specified industry personnel whereby the employee information would be evaluated against local, state, and federal databases to include the Government terrorist threat lists and databases. Initially, industry requested the USSS designate

a red, yellow, or green categorization to the subject signifying the acceptability of their participation at the NSSE. Red applications would be denied, while yellow and green would be accepted. Industry also requested background information on any red applications explaining why the employee was denied access to the NSSE. However, the USSS agreed to send only a yes or no response, and would not include the rationale for disproval of access. The USSS also noted that if an employee with non-national security related outstanding warrants was cleared to attend the NSSE, he/she would be arrested when attempting access. For this reason, the USSS required that each company submit an affidavit signed by the employee, stating that the employee has been advised of this process. The USSS also noted that, due to counterfeiting, they change NSSE badges for each event, and that any personnel supporting such events must be screened separately for each event, even if they have successfully been cleared in the past.

LESSONS LEARNED

The pilot successful highlighted several key lessons for the NSSE industry personnel screening program, such as:

- The USSS will allow NCC member participation in NSSE planning meetings to promote coordination between industry and USSS in preparation for an NSSEs;
- The USSS is best suited to partner with industry and screen industry personnel supporting NSSEs due to their role in planning NSSEs, their standing relationship with industry in screening for NSSEs at the local level, and their access to screening resources;
- The USSS will provide only a yes or no designation for applications requesting access to an NSSE area, and would not provide an explanation to the employee's company;
- Industry personnel requesting this screening must sign an affidavit acknowledging that they are aware of the investigative process due to the possibility that Federal authorities may arrest industry personnel with outstanding warrants as a result of the information gleaned from the screening investigation; and
- The USSS must clear industry personnel prior to each specific NSSE they will be supporting and will not clear a pool of participants to be called on as needed.

In addition, these lessons learned raised further human resources concerns from industry in relation to the information screening program and the lack of information the company will receive on a non-cleared employee:

- What is the best way to handle an individual who has been denied access to an NSSE? Will this person be a threat to their internal systems and business continuity? Where will they reassign this person? In today's environment, there is not a lot of flexibility in assignments.
- Without an explanation as to the reasons for a screening denial, how will the company justify changing an employee's responsibilities?

- What is the potential for a false positive in the identification of an individual?
- Will a denial resulting from a background screening create a negative stigma for the employee?
- Should the screening program be extended to include staff at remote locations responsible for technical support or network design?

As the program progresses and the participants capture and further address lessons learned, the NSTAC will determine whether further TATF action is necessary on this issue.