1. **Purpose.** These guidelines provide the means for DASD(DT&E) staff specialists to engage and assist acquisition program Chief Developmental Testers and Lead DT&E Organizations in developing a robust cybersecurity DT&E strategy. These guidelines are intended to help staff specialists focus on critical developmental issues and measures of cybersecurity to help acquisition programs and decision makers understand cybersecurity risks and improve resilience prior to production and deployment.

2. **Background.** DoD weapons systems and information technologies operate in an increasingly complex, networked, joint information environment. Cybersecurity considerations generally apply to all acquisition systems because they interface to combinations of networks, platforms, support systems, or other elements of the operating environment that are potentially exploitable by cyber threats that are constantly evolving. DoD policy on information assurance IA and the DIACAP are also evolving in response to advances in technology and threat capabilities and will soon transition to cybersecurity under the risk management framework (RMF). These certifications involve assessments of compliance-based security controls and are necessary for establishing a secure foundation; however, they are not sufficient to protect systems in the operational environment from the cyber threat. Programs have also not adequately integrated DIACAP/RMF security controls assessment activities into the TEMP, resulting in incomplete cybersecurity understanding at key acquisition decisions. Developmental test activities should integrate security controls assessments with tests of commonly exploited and emerging vulnerabilities. The TEMP should detail how a program will conduct testing that provides the information needed to assess cybersecurity and inform acquisition decisions. These guidelines should facilitate development and integration of cybersecurity into a comprehensive DT&E strategy documented in the TEMP.

3. **Cybersecurity DT&E Guidelines review and update.** This is version 1.0 of the Cybersecurity DT&E Guidelines. DASD(DT&E) will update these guidelines as major modifications become necessary.

4. **Applicability.** These guidelines are applicable to all major defense acquisition programs (MDAPs), major automated information system (MAIS) programs, and special interest programs designated by the AT&L. Staff specialists should work with Chief Developmental Testers and Lead DT&E Organizations to tailor as appropriate.

5. **Guidelines**

   a. The goal of cybersecurity DT&E is to improve the resilience of military capabilities before beginning production and deployment. Early discovery of system vulnerabilities can facilitate remediation to reduce impact on cost, schedule, and performance. DASD(DT&E) will include an evaluation of cybersecurity in DAES reviews and DT&E Assessments provided at major decision points.
b. Figure 1 depicts the cybersecurity DT&E process mapped to the acquisition life cycle. The cybersecurity DT&E process is a continuum of activities from pre-Milestone A to cybersecurity DT&E in support of Milestone C. The steps may apply to different phases of the acquisition life cycle depending upon the phasing of program engineering and production activities. The process is intended to translate cybersecurity requirements, host environment, threat, and other considerations into tests designed to improve understanding of cybersecurity risks to the mission and to develop measures to improve resilience of military capabilities.

![Cybersecurity DT&E process mapped to the Acquisition Life Cycle](image)

**Figure 1. Cybersecurity DT&E process mapped to the Acquisition Life Cycle**

c. The cybersecurity DT&E process consists of four steps: the first two steps are generally an analysis of the system requirements, design, operating environment, and early test artifacts; the third step is focused on identifying and closing vulnerabilities; and the fourth step is cybersecurity DT&E in a representative environment against a robust cyber threat to confirm readiness for production. Steps 1–3 identify the specified, implied, and essential tasks necessary to improve cybersecurity in support of mission accomplishment. Specified tasks consist of documented cybersecurity requirements; implied tasks include additional tasks the developer must accomplish to operate securely in the operational environment; and essential tasks are those that must be achieved to provide sufficient resilience to support mission accomplishment in the presence of cyber attack. This analysis is critical to focus Step 4 cybersecurity DT&E on identifying remaining vulnerabilities so the developer can take corrective actions before production and deployment.

d. DASD(DT&E) staff specialists, working with the T&E WIPT, should seek opportunities to improve efficiency by integrating cybersecurity into other planned DT&E events. Historically, TEMPs and associated test plans have not adequately addressed cybersecurity measures or resources, such as cyber ranges. A dedicated cybersecurity test event, such as testing in a cyber range, may be necessary to overcome limitations to testing on the live network.

---

1 The idea of specified, implied, and essential tasks is analogous to the mission analysis in the military decision-making process (see Joint Publication 5-0).
The following paragraphs describe each step in the cybersecurity DT&E process. Table 1 summarizes the critical developmental issues and measures of cybersecurity during DT&E. Appendix 1 provides suggested TEMP review items and example language. Appendix 2 identifies commonly exploited vulnerabilities that should be included in cybersecurity test plans as appropriate. DAS(DT&E) staff specialists should tailor application of these guidelines as appropriate for each program.

**Step 1: Understand Cybersecurity Requirements.** This step is an analysis of system documentation to identify specified cybersecurity requirements. Staff specialists should perform a thorough examination of system documents, such as the JCIDS ICD/CDD/CPD, SEP, Program Protection Plan (PPP), Information Assurance Strategy (IAS), Information Support Plan (ISP), System Threat Assessment Report (STAR), and others, to identify system cybersecurity requirements. Staff specialists will use this analysis to assist programs in developing an executable cybersecurity DT&E strategy documented in the TEMP.

Staff specialists should engage the Chief Developmental Testers and Lead DT&E Organizations to accomplish the following:

- Identify cybersecurity requirements for DT&E. These should include mitigation of applicable common vulnerabilities listed in Appendix 2.
- Integrate cybersecurity into DT&E events and/or plan for dedicated cybersecurity test events as appropriate.
- Identify cybersecurity test organization(s), including:
  - DIACAP/RMF security controls assessor
  - Blue Team² (during DT&E, the Blue Team may be a Government organization or contractor equivalent)
  - Red Team³ (during DT&E, the Red Team may be a National Security Agency (NSA)-certified Government organization or contractor equivalent)
- Identify cyber threats to be emulated in test.
- Identify MAC/CL or risk category.
- Identify cybersecurity DT&E resources:
  - Cyber range resources (e.g., National Cyber Range (NCR), DoD IA Range, Joint Information Operations Range (JIOR))
  - M&S or tools for cybersecurity

---

² Blue Team – A group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer’s cybersecurity readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer’s networks are as secure as possible before having the Red Team test the systems. (IA Glossary, NIST CNSSI 4009)

³ Red Team – A group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The Red Team’s objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. (IA Glossary, NIST CNSSI 4009)
Step 2: Characterize the Cyber Attack Surface. The objective of Step 2 is to characterize the cyber attack surface to identify the additional implied cybersecurity requirements. System interfaces collectively contribute to the overall attack surface. The attack surface may be defined as the system’s exposure to reachable and exploitable vulnerabilities; in other words, any connection, data exchange, service, removable media, etc., may expose the system to potential threat access. Programs should not assume delivered support components GFE, CFE, COTS, PARM systems, etc.) are risk free; the system is only as secure as its weakest link. Staff specialists should assist the program to accomplish the following during Step 2:

- Examine system architecture products (e.g., SV-1, SV-6 viewpoints) to identify interfacing systems, services, and data exchanges that may expose the system to potential threat exploits.
- Examine system CONOPS to understand roles and responsibilities of system operators, administrators, and the Computer Network Defense Service Provider (CNDSP).
- Identify host environment provisions for system protection, monitoring, access control, system updates, etc.
- Utilize cybersecurity SMEs to assist in analyzing the attack surface to determine likely avenues of cyber attack.
- Evaluate early DIACAP/RMF and other security test artifacts.

Step 3: Understand the Cyber Kill Chain. Understanding how the cyber adversary may obtain access (the attack surface) is critical to determine potential actions the adversary may take. The cyber kill chain is as a sequence of activities and events used by a threat to execute a cyber attack. Although there are variations of the kill chain, the typical stages include reconnaissance, weaponize, deliver, exploit, control, execute, and maintain. Step 3 involves an analysis of potential kill chain activities to identify essential cybersecurity requirements necessary to improve resilience of the operational system to cyber attack. A Blue Team performs a vulnerability assessment of the system and its interfaces and conducts cybersecurity testing during system integration tests to identify vulnerabilities for corrective action. Staff specialists work with the program to accomplish the following during Step 3:

- Develop initial concept for contractor and Government cybersecurity testing activities at the component and subsystem level.
  - Identify test opportunities in which representative systems and services will be available to conduct cybersecurity testing in a system-of-systems context (such as JITC interoperability testing).
  - Identify and integrate DIACAP/RMF security controls assessment activities into unit testing, functional testing, etc.
  - Evaluate early DIACAP/RMF artifacts.
- Perform a vulnerability assessment, using a Blue Team, to determine likely avenues of cyber attack and the most likely threat exploits (see examples at Appendix 2).
  - Include or emulate the CNDSP.
  - Blue Team scans systems and interfaces to determine potential cyber kill chain activities.
• Analyze the kill chain to determine how the system would respond in the contested cyber domain.

Staff specialists should work with the program to use Steps 2 and 3 analysis to refine the scope and objectives for Step 4 cybersecurity DT&E, and incorporate into the MS B TEMP. This analysis will also be useful in assigning responsibility for any vulnerability discovered in testing to the materiel developer, user, host environment, or CNDSP.

**Step 4: Cybersecurity DT&E.** Step 4 evaluates system cybersecurity in a mission context, using realistic threat exploitation techniques. A Red Team performs rigorous cybersecurity testing in a system-of-systems environment. Depending on risk, Step 4 testing may involve the use of a cyber range to reduce the risk of collateral damage to live networks and authoritative data sources. The following activities are accomplished during Step 4:

• Conduct Red Team assessment to identify remaining vulnerabilities.
  – Include or emulate the CNDSP.
  – Include typical users if available.
  – Red Team attempts to exploit the attack surface and execute cyber kill chain activities.
• Identify exploitable threat vectors and vulnerabilities (see examples at Appendix 2).
• Analyze results to determine impact to mission.
• Recommend corrective actions to improve resilience.
  – May include non-materiel solutions such as tactics, techniques, and procedures (TTP) and recommendations to the CNDSP.

The cybersecurity DT&E process may be an iterative process. Staff specialists should be cognizant of configuration changes, software and hardware updates, and incremental development activities that deliver new features on a recurring basis that may necessitate follow-on requirements, attack surface, and kill chain analysis, and cybersecurity DT&E.

Table 1 summarizes the key considerations for each step of the cybersecurity DT&E process.
Table 1. Cybersecurity DT&E Process Summary

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Understand Cybersecurity Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Step 1 analysis should answer the following:</td>
</tr>
<tr>
<td></td>
<td>• What are the specified cybersecurity requirements?</td>
</tr>
<tr>
<td></td>
<td>• What are the critical missions, functions, and components?</td>
</tr>
<tr>
<td></td>
<td>• What are the cybersecurity threats?</td>
</tr>
<tr>
<td></td>
<td>• Is the DIACAP/RMF package initiated with MAC/CL or a risk category assigned?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Characterize the Attack Surface</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Analysis and DT&amp;E conducted during Step 2 should answer the following:</td>
</tr>
<tr>
<td></td>
<td>• What are the key interfacing systems and services?</td>
</tr>
<tr>
<td></td>
<td>• What potential vulnerabilities are introduced by the operating and host environment?</td>
</tr>
<tr>
<td></td>
<td>• What protections and monitoring capabilities are provided by host environment and CNDSP?</td>
</tr>
<tr>
<td></td>
<td>• What additional implied cybersecurity requirements does the operating and host environment introduce?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Understand the Cyber Kill Chain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Analysis and DT&amp;E conducted during Step 3 should answer the following:</td>
</tr>
<tr>
<td></td>
<td>• What are the likely kill chain activities should an adversary gain access to the system?</td>
</tr>
<tr>
<td></td>
<td>• What potential vulnerabilities (see Appendix 2) are likely to be exploited?</td>
</tr>
<tr>
<td></td>
<td>• What are the results of initial DIACAP/RMF security controls assessment?</td>
</tr>
<tr>
<td></td>
<td>– What are the CAT I and CAT II vulnerabilities*?</td>
</tr>
<tr>
<td></td>
<td>• What are the results of the Blue Team scans and what are the recommended corrective actions?</td>
</tr>
<tr>
<td></td>
<td>• What essential cybersecurity requirements must be met to mitigate operational impacts of the cyber kill chain?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Cybersecurity DT&amp;E</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DT&amp;E conducted during Step 4 should answer the following:</td>
</tr>
<tr>
<td></td>
<td>• What are the final results of the DIACAP/RMF security controls assessment?</td>
</tr>
<tr>
<td></td>
<td>– Have all CAT I and CAT II vulnerabilities* been resolved?</td>
</tr>
<tr>
<td></td>
<td>– Is there a plan and schedule for remediating critical unresolved vulnerabilities?</td>
</tr>
<tr>
<td></td>
<td>– If mitigation or remediation efforts have been completed, have they been tested and included in the DT evaluation report?</td>
</tr>
<tr>
<td></td>
<td>• What are the results of the Red Team penetration test?</td>
</tr>
<tr>
<td></td>
<td>– What kill chain activities was the Red Team successful in implementing?</td>
</tr>
<tr>
<td></td>
<td>– What common vulnerabilities were successfully exploited (see Appendix 2)?</td>
</tr>
<tr>
<td></td>
<td>– What were the test limitations?</td>
</tr>
<tr>
<td></td>
<td>• How resilient is the system to cyber attack when supporting mission operations?</td>
</tr>
<tr>
<td></td>
<td>• What are the recommended corrective actions?</td>
</tr>
<tr>
<td></td>
<td>– for the PM?</td>
</tr>
<tr>
<td></td>
<td>– for the user?</td>
</tr>
<tr>
<td></td>
<td>– for the host environment and/or CNDSP?</td>
</tr>
<tr>
<td></td>
<td>• When should the next cybersecurity tests occur in support of new capability development and/or threat assessment?</td>
</tr>
</tbody>
</table>

* Severity categories are assigned to a system weakness or shortcoming by a certifying authority (CA) or a designated representative as part of a certification analysis to indicate the risk level associated with the security weakness and the urgency with which the corrective action must be completed. Severity categories are expressed as category (CAT) I, CAT II, and CAT III. Severity categories are assigned after considering all possible mitigation measures that have been implemented within system design and architecture limitations for the DoD information system (IS) in question. For instance, what may be a CAT I weakness in a component part of a system (e.g., a workstation or server) may be offset or mitigated by other protections within hosting enclaves so that the overall risk to the system is reduced to a CAT II.

• CAT I weaknesses shall be corrected before an authorization to operate (ATO) is granted.
• CAT II weaknesses shall be corrected or satisfactorily mitigated before an ATO can be granted.
• CAT III weaknesses will not prevent an ATO from being granted if the DAA accepts the risk associated with the weaknesses.

Appendix 1

Cybersecurity DT&E in the Test and Evaluation Master Plan

This Appendix is intended to be a resource to help DASD(DT&E) Staff Specialists review TEMPs for cybersecurity, with emphasis on the MS B TEMP. The outline is based upon the current TEMP template in the Defense Acquisition Guidebook. Cybersecurity does not need to be addressed in every section, and every program will address cybersecurity differently; staff specialists should assist programs in developing the appropriate sections of the TEMP to ensure that cybersecurity DT&E is adequately addressed. Example TEMP statements are provided.

1. PART I

1.3.1. System Threat Assessment. Review this section to determine whether the threat discussed here is adequately portrayed in the DT&E events in Part III and resources in Part IV.

  *Example TEMP Statement:* The DT&E and OT&E events described in Part III will include cybersecurity T&E consistent with the cybersecurity threats described in the System Threat Assessment Report (STAR).

1.3.2.1. Previous Testing and Results. Review this section and ensure that the results of any previous cybersecurity tests that will affect the T&E strategy are discussed. For example, a previous system increment may have received approval to operate but deferred correction of CAT II cybersecurity weaknesses to the current increment. Ensure that the DT&E events discussed in Part III include tests to verify corrections of these deficiencies.

1.3.3. Key Capabilities. Review this section to ensure that cybersecurity-related KPPs and key KSAs for the system are included. Current IA policy identifies DIACAP requirements. The system may be categorized as Platform Information Technology (PIT), or assigned a MAC and CL. The MAC should be identified as I, II, or III; CL should be identified as Public, Sensitive but Unclassified, or Classified. Future cybersecurity policy will establish the Risk Management Framework requirements and replace MAC and CL with Risk Categories, and treat PIT in the same manner as other IT.

1.3.3.1. Key Interfaces. Review this section and identify interfaces with existing or planned system architectures required to accomplish critical operational missions. These key interfaces are part of the “attack surface.” Most systems interoperate with other systems and inherit some cyber-defense mechanisms from a supporting network. Ensure that the DT&E events described in Part III and resources in Part IV include the relevant interfacing systems and CNDSP.

  *Example TEMP Statement:* Cybersecurity DT&E will include interfacing systems and supporting services to characterize the attack surface to identify and mitigate vulnerabilities. The Tier 1 CNDSP is xxx; Tier 2 CNDSP is yyy; Tier 3 CNDSP is zzz.

1.3.3.2. Special Test or Certification Requirements. Review this section to identify additional evaluation requirements. The PPP may identify the need for anti-tamper certifications.
1.3.3.3. Systems Engineering (SE) Requirements. Review this section to ensure that the critical documents that establish cybersecurity engineering requirements are addressed. Key documents of interest include systems specifications, preliminary and critical designs, PPP, and SEP.

2. PART II

2.1. T&E Management. Review this section to ensure that it describes how cybersecurity DT&E will be managed as part of existing T&E management processes and procedures. Ensure that the key management roles that include the DIACAP/RMF security controls assessor, Blue Team, and Red Team, are addressed.

2.1.1. T&E Organizational Construct. Review this section to ensure that responsibilities for cybersecurity T&E are identified clearly and key members are identified as part of the T&E WIPT, including DIACAP/RMF security controls assessor, Blue Team, and Red Team.

2.3. Deficiency Reporting. Review this section to understand how T&E deficiencies will be reported. Deficiencies identified during cybersecurity T&E may be classified and/or may not be attributed to the SUT. Review this section to ensure that results of cybersecurity T&E are available to all stakeholders as necessary. Special handing may be required.

2.5. Integrated Test Program Schedule. Review the schedule to identify cybersecurity DT&E activities. Cybersecurity DT&E should be integrated with other planned DT&E events but may include dedicated events such as Red Team testing in a cyber range. Ensure that the DT&E events described in Part III and resources in Part IV adequately address the cybersecurity DT&E activities shown in the integrated test program schedule.

3. PART III

3.3. Developmental Evaluation Approach. Review this section to ensure that cybersecurity is an integral part of the overall T&E strategy. The Chief Developmental Tester and Lead DT&E Organization should be planning to address cybersecurity requirements that may be in addition to DIACAP/RMF certification activities during cybersecurity DT&E.

Example TEMP Statement: 3.3.X. Cybersecurity DT&E Strategy. Cybersecurity DT&E will be executed in conjunction with other DT&E activities or as dedicated events as necessary. Cybersecurity DT&E events include Blue Team assessments to scan for common vulnerabilities and Red Team penetration events to replicate the threat consistent with the STAR.

3.3.2. Developmental Test Objectives. Review the event descriptions in this section to ensure that DT&E events identified in the integrated test program schedule are adequately scoped to support program decisions.
Early DT&E Events
Cybersecurity DT&E activities at the “Step 2 level” may be integrated into DT&E activities for components and subsystems to confirm compliance with technical specifications. IA controls testing for components and integrated subsystems shall be performed based upon the assigned MAC/CL or RMF risk category. This testing may be accomplished by the contractor with Government oversight or by the DIACAP/RMF security controls assessor.

Intermediate DT&E Events
Cybersecurity DT&E activities at the “Step 3 level” may be integrated into DT&E activities to verify system functionality in a relevant cyber environment. A Blue Team vulnerability assessment should be conducted to identify potential vulnerabilities, when the system is supported by the CNDSP (the CNDSP may be simulated), which if successfully exploited, may adversely affect system performance, data integrity, and mission accomplishment.

Example TEMP Statement:
T&E Objectives. A formal Blue Team vulnerability assessment will be conducted to identify potentially exploitable vulnerabilities. The security controls assessor will confirm compliance with applicable IA controls.

Event, Scope of Testing, and Scenarios. Early vulnerability assessments may be conducted against critical designs. Testing shall include unit testing, static code analysis, STIG compliance, DIACAP/RMF compliance, and vulnerability assessment activities. Blue Teams will examine the cyber attack surface to identify potential vulnerabilities and to determine corrective actions necessary for the system to sustain critical operational missions in a contested cyber domain.

Test Limitations. Testing cannot be conducted in the operational environment due to real world considerations. Therefore, testing shall be conducted in a Systems Integration Lab (SIL).

Cybersecurity DT&E
Step 4 cybersecurity DT&E may require a cyber range to prevent collateral damage to other systems, services, and data sources. Cybersecurity DT&E shall verify mechanisms used to protect the system, including inherited protections from the CNDSP and/or host systems. Red Teams will attempt to execute the cyber kill chain to evaluate mission impacts and to determine corrective actions necessary for the system to sustain critical missions in a contested cyber domain. The system’s resiliency and ability to detect, deny, deceive/redirect, disrupt, degrade, and recover in response to cyber-attacks should be understood. Cyber threats shall be portrayed consistent with the STAR. The T&E infrastructure may include simulated network conditions and interfacing systems.

Example TEMP Statement:
T&E Objectives. Evaluate system cybersecurity mechanisms by replicating attempted compromises in a contested cyber domain. The objective is to understand system resiliency and ability to detect, deny, deceive/redirect, disrupt, degrade, and recover in response to cyber-attacks.
Event, Scope of Testing, and Scenarios. T&E shall verify cybersecurity mechanisms used to protect critical data exchanges and inherited protections from the CNDSP and/or host systems. The Red Team will attempt to execute the cyber kill chain through penetration and exploitation testing in a mission context and realistic cyber environment to evaluate mission impacts. Cyber threats shall be portrayed consistent with the STAR.

Test Limitations. The cyber range is an approximation of the operational environment using simulated services, virtual machine interfaces, and simulated traffic.

3.3.4. Test Limitations. Describe any limitations to performing cybersecurity DT&E. Describe any limitations to using an operationally realistic mission environment that includes representative users and cyber ranges.

Section 3.7. Other Certifications. The TEMP may describe other certifications that may affect cybersecurity T&E, including Platform IT, DIACAP/RMF, and interoperability certifications.

Example TEMP Statement:
DIACAP/RMF IATT/IATO/ATO Certifications: Certification test results and test data will be available for review by the T&E WIPT and used in the assessment to inform the MDA in support of the MSC decision.

4. PART IV
Ensure that Part IV specifies the resources necessary to accomplish cybersecurity DT&E, including Blue and Red Teams, CNDSP, test sites (host environments), M&S, special equipment and instrumentation, and use of a cyber range.
Appendix 2

Common Exploitable Vulnerabilities

Password Practices
- Use of well-known default passwords on devices and software (failure to change default passwords)
- Poor user password practices (contrary to policy guidance)
- Improperly secured user identification (UID) and password lists stored and readable from the trusted network
- Passwords stored on network devices without encryption or with weak encryption
- Use of keyboard pattern password
- Pass-the-Hash exploit (Microsoft Active Directory vulnerability)
- Login credential discovered during Web searches (reconnaissance)

Privileged Access
- Standard user credentials with administrative privileges granted
- Use of shared administrator accounts
- Administrator accounts using identical UID/passwords across multiple server platforms
- Administrators using privileged accounts to access Internet Web servers
- Administrators using privileged accounts continuously

Access Control
- Use of unsecure ports and protocols (Port 80: HTTP)
- Use of prohibited ports and protocols
- Unsecure network services enabled on network devices and systems
- Secure Sockets Layer (SSL) vulnerabilities accepting invalid certificates
- Anonymous File Transfer Protocol (FTP) allowed
- Lack of Access Control Lists (ACLs) implemented on border router
- Phishing emails with SSL exploits

Computer Network Defense Service Provider (CNDSP) Monitoring and Operations
- Inadequate detection of insertion of removable media (host-based security system (HBSS))
- HBSS misconfiguration
- HBSS not monitored properly
- Unauthorized (rogue/malicious) devices installed on network not detected
- Use of physical intrusion devices not detected
- Unauthorized software installed on workstations not detected (HBSS)
- Misconfigured Intrusion Detection Systems (IDS)
- IDS not properly monitored
- Ineffective use of system audit logs
- Data exfiltrations not detected
- Poor incident handling procedures
- Lack of Tier 3 network defense collaboration cell
Workstations and Server Configurations

- Insecure configurations for hardware and software on mobile devices, laptops, workstations, and servers (noncompliant remediation of known vulnerabilities)
- Unpatched server and workstation vulnerabilities (Buffer Overflow and Code Injection Vulnerabilities)
- Use of unauthorized software
- Unreliable software base-lining practices (lack of adequate configuration management (CM))
- SharePoint server insecure/noncompliant configuration (unauthenticated, unrestricted access to files)
- SharePoint server failure to implement AV scanning for file uploads
- Unsecured SharePoint server
- Noncompliance with software and hardware backup requirements
- Misconfigured services and vulnerable drivers
- Misconfigured servers
- Network credentials, system configurations, and network diagrams stored insecurely
- Web application vulnerable to Standard Query Language (SQL) injection attack (input validation vulnerability)
- Unauthorized data manipulation, due to weak data protections
- Operational information stored insecurely (no authentication or encryption used)
- Unsecured chat systems

Infrastructure

- No Wireless Intrusion Detection (WIDS) devices implemented
- Logging for infrastructure (network) devices not implemented
- Layer 2 VLAN software vulnerable (unpatched)
- Exploitation of two-way trust relationship between domains
- Physical Security of critical components