|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}**  **eMASS# {EMASS#}**  **Confidentiality: {CONFIDENTIALITY}**  **Integrity: {INTEGRITY}**  **Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Incident Response Plan**  **Document Version: 1.0.0**  **{DATE}** |
| Prepared by: {ORGANIZATION}  **DISTRIBUTION IS LIMITED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS.**  **OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO:** {ORGANIZATION} |

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Changes Made / Section(s) |
| {DATE} | 1.0.0 | {ACRONYM} | Initial Document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Amplifying Guidance**

1. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, "Cyber Incident Handling Program" [PDF icon](http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf)
2. NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide" [PDF icon](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)
3. United States Cyber Command [](https://www.cybercom.mil/default.aspx)
4. United States Computer Emergency Readiness Team [](https://www.us-cert.gov/)

**Table** **of Contents**

[1.0 OVERVIEW 1](#_Toc432593094)

[1.1 Applicability 1](#_Toc432593095)

[1.2 Internal Roles and Points of Contact 2](#_Toc432593096)

[2.0 INTRODUCTION 3](#_Toc432593097)

[3.0 CYBER INCIDENT HANDLING PROCESS AND LIFE CYCLE 4](#_Toc432593098)

[3.1 Detection of Events 4](#_Toc432593099)

[3.2 Preliminary Analysis and Identification 5](#_Toc432593100)

[3.2.1 Preliminary Analysis and Identification Methodology 6](#_Toc432593101)

[3.3 Preliminary Response Actions 7](#_Toc432593102)

[3.3.1 Preliminary Response Action Methodology 7](#_Toc432593103)

[3.4 Incident Analysis 8](#_Toc432593104)

[3.4.1 Incident Analysis Methodology 9](#_Toc432593105)

[3.5 Response and Recovery 11](#_Toc432593106)

[3.5.1 Response and Recovery Methodology 11](#_Toc432593107)

[3.6 Post-Incident Analysis 13](#_Toc432593108)

[4.0 INFORMATION SPILLS 13](#_Toc432593109)

[APPENDIX A – CYBER INCIDENT AND REPORTABLE CYBER EVENT CATEGORIZATION 15](#_Toc432593110)

[APPENDIX B – CYBER INCIDENT REPORTING 18](#_Toc432593111)

[APPENDIX C – GENERAL CYBER INCIDENT REPORT FORMAT 23](#_Toc432593112)

[APPENDIX D – DELIVERY VECTORS 27](#_Toc432593113)

[APPENDIX E – IMPACT ASSESSMENT MATRIX 30](#_Toc432593114)

[APPENDIX F – COORDINATION AND DE-CONFLICTION 32](#_Toc432593115)

[APPENDIX G – LESSONS LEARNED / AFTER ACTION REPORTS 34](#_Toc432593116)

[G.1.0 LESSONS LEARNED 35](#_Toc432593117)

[G.2.0 AFTER ACTIONS REPORTS 35](#_Toc432593118)

[G.3.0 METRICS 36](#_Toc432593119)

[APPENDIX H – INCIDENT RESPONSE PLAN TESTING 38](#_Toc432593120)

[APPENDIX I – DETAILED COMPLIANCE MATRIX 42](#_Toc432593121)

[ENCLOSURE 1 – AFTER ACTIONS REPORT TEMPLATE 68](#_Toc432593122)

[ENCLOSURE 2 – TRAINING RESOURCES 70](#_Toc432593123)

[Incident Response 71](#_Toc432593124)

[Data Spills 71](#_Toc432593125)

[Administrative Inquiry 71](#_Toc432593126)

[Insider Threat Training 71](#_Toc432593127)

[Insider Threat Job Aids 72](#_Toc432593128)

[Insider Threat Best Practices 72](#_Toc432593129)

[Figure 1 - Cyber Incident Lifecycle 4](#_Toc432432559)

[Figure 2 - Preliminary Analysis and Identification Methodology 6](#_Toc432432560)

[Figure 3 - Prelimenary Response Actions 7](#_Toc432432561)

[Figure 4 - Incident Analysis Methodology 9](#_Toc432432562)

[Figure 5 - Response and Recovery Methodology 12](#_Toc432432563)

[Table 1 - SP-800-53v4 Compliance Matrix 1](#_Toc432508950)

[Table 2 - Computer Network Defense Service Providers 2](#_Toc432508951)

[Table 3 - Internal Roles and Points of Contact 3](#_Toc432508952)

[Table 4 - Category Precedence 16](#_Toc432508953)

[Table 5 - Cyber Incident and Reportable Cyber Event Categories 17](#_Toc432508954)

[Table 6 - Incident Report Vehicles 19](#_Toc432508955)

[Table 7 - Incident Reporting Timelines 22](#_Toc432508956)

[Table 8 - Report Format 26](#_Toc432508957)

[Table 9 - Delivery Vectors 29](#_Toc432508958)

[Table 10 - Impact Levels 31](#_Toc432508959)

# **OVERVIEW**

A Cyber Incident is defined as, “An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Guidance contained herein will cover the high-level procedures related to the Protect, Monitor, Analyze, Detect, and Respond phases of the Computer Network Defense (CND) life cycle. It will describe the policies and processes required to operate a comprehensive DoD cyber incident-handling program. More specific guidance tailored for the individual requirements of CC/S/A/FAs will be provided through operation orders (OPORDs), warning orders (WARNORDs), fragmentary orders (FRAGOs), tasking orders (TASKORDs), or similar command authority orders and directives. This document is a framework that will be used by {ACRONYM} and individuals to provide a unified approach to cyber incident handling to enable effective collaboration between and across DoD distributed organizations in a way that improves the {ACRONYM}’s ability to protect and defend DoD information networks and information.

This document complies with the following requirements from NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations". A detailed compliance matrix can be found in [Appendix I, “Detailed Compliance Matrix”](#_APPENDIX_I_–).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| [IR-1](#IR1) | Incident Response Policy and Procedures | P1 | IR-1 | IR-1 | IR-1 |
| [IR-2](#IR2) | Incident Response Training | P2 | IR-2 | IR-2 | IR-2 (1) (2) |
| [IR-3](#IR3) | Incident Response Testing | P2 | Not Selected | IR-3 (2) | IR-3 (2) |
| [IR-4](#IR4) | Incident Handling | P1 | IR-4 | IR-4 (1) | IR-4 (1) (4) |
| [IR-5](#IR5) | Incident Monitoring | P1 | IR-5 | IR-5 | IR-5 (1) |
| [IR-6](#IR6) | Incident Reporting | P1 | IR-6 | IR-6 (1) | IR-6 (1) |
| [IR-7](#IR7) | Incident Response Assistance | P2 | IR-7 | IR-7 (1) | IR-7 (1) |
| [IR-8](#IR8) | Incident Response Plan | P1 | IR-8 | IR-8 | IR-8 |
| [IR-9](#IR9) | Information Spillage Response | P0 | Not Selected | Not Selected | Not Selected |
| [IR-10](#IR10) | Integrated Information Security Analysis Team | P0 | Not Selected | Not Selected | Not Selected |

Table - SP-800-53v4 Compliance Matrix

## **1.1 Applicability**

This IRP contains information that is required to present the full incident lifecycle and reporting requirements. The {ACRONYM} role within this process is Tier III, which initiates local operational reporting and receives support from and responds to direction from a designated Tier II Computer Network Defense Service Provider (CNDSP). The {ACRONYM} CNDSPs are:

**DELETE N/A CNDSP**

|  |  |  |  |
| --- | --- | --- | --- |
| Network / System | Provider | Phone/Fax | Email |
| Secret Internet Protocol Router Network (SIPRNet) | Navy Cyber Defense Operations Command (NCDOC)  <https://www.ncdoc.navy.mil>  <http://www.ncdoc.navy.smil.mil> | DSN: (312) 537-4024 Com: (757) 417-4024  Toll: (888) 628-2362  STE: (312) 537-7952  STE: (757) 417-7952 | [ncdoc@ncdoc.navy.mil](mailto:ncdoc@ncdoc.navy.mil)  [cndwo@ncdoc.navy.smil.mil](mailto:cndwo@ncdoc.navy.smil.mil)  Plain Language Address: NCDOC NORFOLK VA |
| Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) | Navy Cyber Defense Operations Command (NCDOC)  <https://www.ncdoc.navy.mil>  <http://www.ncdoc.navy.smil.mil> | DSN: (312) 537-4024 Com: (757) 417-4024  Toll: (888) 628-2362  STE: (312) 537-7952  STE: (757) 417-7952 | [ncdoc@ncdoc.navy.mil](mailto:ncdoc@ncdoc.navy.mil)  [cndwo@ncdoc.navy.smil.mil](mailto:cndwo@ncdoc.navy.smil.mil)  Plain Language Address: NCDOC NORFOLK VA |
| Non-GiG Connected | Navy Cyber Defense Operations Command (NCDOC)  <https://www.ncdoc.navy.mil>  <http://www.ncdoc.navy.smil.mil> | DSN: (312) 537-4024 Com: (757) 417-4024  Toll: (888) 628-2362  STE: (312) 537-7952  STE: (757) 417-7952 | [ncdoc@ncdoc.navy.mil](mailto:ncdoc@ncdoc.navy.mil)  [cndwo@ncdoc.navy.smil.mil](mailto:cndwo@ncdoc.navy.smil.mil)  Plain Language Address: NCDOC NORFOLK VA |
| Defense Research and Engineering Network (DREN) | High Performance Computing Modernization Program (HPCMP)  <https://www.hpc.mil> | Com: (703) 812-8205 | [hpccert@cert.hpc.mil](mailto:hpccert@cert.hpc.mil) |
| Secret Defense Research Engineering Network (SDREN) | High Performance Computing Modernization Program (HPCMP)  <https://www.hpc.mil> | Com: (703) 812-8205 | [hpccert@cert.hpc.mil](mailto:hpccert@cert.hpc.mil) |

Table - Computer Network Defense Service Providers

## **1.2 Internal Roles and Points of Contact**

A single incident response team has been created to handle incidents throughout {ACRONYM}. The team has only part-time incident response team members, serving as more of a virtual incident response team. When an emergency occurs, the team members are contacted rapidly, and those who can assist do so. The IT help desk acts as a first point of contact for incident reporting. The help desk members are trained to perform the initial investigation and data gathering and then alert the incident response team if it appears that a serious incident has occurred. The following roles have been established for the {ACRONYM} Incident Response Team:

| Role | Responsibility | Point of Contact |
| --- | --- | --- |
| Management | Establishes incident response policy, budget, and staffing. Ultimately, management is held responsible for coordinating incident response among various stakeholders, minimizing damage, and reporting. | {NAME}  {PHONE}  {EMAIL} |
| Information Systems Security Manager (ISSM) | Information security staff members may be needed during certain stages of incident handling (prevention, containment, eradication, and recovery)—for example, to alter network security controls (e.g., firewall rulesets). | {NAME}  {PHONE}  {EMAIL} |
| IT Support | IT technical experts (e.g., system and network administrators) not only have the needed skills to assist but also usually have the best understanding of the technology they manage on a daily basis. This understanding can ensure that the appropriate actions are taken for the affected system, such as whether to disconnect an attacked system. | {NAME}  {PHONE}  {EMAIL} |
| Physical Security | Some computer security incidents occur through breaches of physical security or involve coordinated logical and physical attacks. The incident response team also may need access to facilities during incident handling—for example, to acquire a compromised workstation from a locked office. | {NAME}  {PHONE}  {EMAIL} |

Table - Internal Roles and Points of Contact

# **INTRODUCTION**

The methodology described in this section provides a general, standardized process that establishes the intent and requirements for detecting, analyzing, and responding to information or technology events or cyber incidents for the purpose of mitigating any adverse operational or technical impact on DoD data, ISs, and information networks.

An effective cyber incident handling capability relies on disciplined processes, procedures, and ISs. These must communicate timely, accurate, and accessible information about the cyber incident’s cause, impact, and current situation to incident responders, command authorities, and others involved in directing incident response actions. The primary objectives of this cyber incident handling process is to:

1. Maintain a robust detection capability to ensure all suspicious activity is detected and reported so that further analysis can take place to determine if it is a reportable cyber event or incident.
2. Ensure the timely reporting of cyber incidents through appropriate technical and operational channels in a way that promotes an accurate, meaningful, and comprehensive understanding of the cyber incident throughout its life cycle.
3. Effectively contain events and incidents and isolate ISs to minimize any damage or impact to DoD information networks, ISs, data, and services.
4. Safely acquire and preserve the integrity of data required for cyber incident analysis to help determine the technical/operational impact, root cause(s), scope, and nature of the cyber event or incident.
5. Ensure the effective coordination and communication of cyber incident information through appropriate channels and with appropriate stakeholders, higher CND organizations, and/or CC/S/A/FAs’ headquarters (HQ).
6. Provide an effective and comprehensive response that includes the recovery of any affected ISs and the return to a fully functioning, secure, operational state for all services and ISs.
7. Identify lessons learned to help improve infrastructure component protection strategies and cyber incident handling procedures to prevent a recurrence of the cyber event or incident. Observations should be entered into the Joint Lessons Learned Information System (JLLIS) at http://www.jllis.smil.mil. JLLIS is the DoD system of record for lessons learned. Use of JLLIS allows for the dissemination of lessons learned throughout the Joint Force.
8. Understand patterns of activity and trends to characterize the threat and direct protective and defensive strategies.

# **3.0 CYBER INCIDENT HANDLING PROCESS AND LIFE CYCLE**

The basic process for DoD cyber incident handling can be grouped into the following processes or phases:

1. Detection of events.
2. Preliminary analysis and identification of incidents.
3. Preliminary response actions.
4. Incident analysis.
5. Response and recovery.
6. Post-incident analysis.



Figure - Cyber Incident Lifecycle

What is learned throughout the process can be leveraged to improve the state of the practice in defending against future attacks.

## **3.1 Detection of Events**

Detection of cyber events is the continuous process of identifying any unusual network or IS activity that has the potential to adversely affect DoD information networks, ISs, or operational missions. The primary objectives of detecting cyber events include:

1. Ensuring all suspicious activity is detected and reported so that further analysis can take place to determine if it is a reportable cyber event or incident.
2. Ensuring suspicious activity is reported in a timely manner consistent with required reporting timelines.
3. Effectively coordinating with command channels and other DoD organizations.

As part of this process, information about potential incidents, vulnerabilities, or other security or incident information is gathered and reported to the appropriate area for analysis and response. This process is important because it is the point where an anomalous or unusual cyber event is first noticed and identified as something that must be reviewed. It may also be the first point at which a cyber event is reported. Detection starts the reporting process Detection of a cyber event may occur in various ways, including by:

1. An automated detection system or sensor.
2. A report from an individual or user.
3. An incident report or situational awareness update from other internal or external organizational components, such as other CNDSPs, USCYBERCOM, US-CERT, IC, LE/CI, or other external Computer Security Incident Response Team entities.

## **3.2 Preliminary Analysis and Identification**

Performing preliminary analysis and identifying incidents is the process of performing initial analysis of a detected cyber event to determine if it is a reportable cyber event or incident. The primary objectives for this phase include the following:

1. Determining whether a detected event is a reportable cyber event or incident.
2. Ensuring all appropriate DoD organizations are notified through technical and operational reporting channels.
3. Ensuring the timely submission of an initial incident report that contains as much complete and useful information as is available (or possible).

A standardized benchmark is used for defining a reportable cyber event or incident. If an event does not meet the incident criteria, it can be removed from consideration. If the proper preliminary analysis is not done, some incidents may not be identified and therefore never be reported. Such a failure can impact the global security posture of the DoD information networks, resulting in an inaccurate operational picture and potentially allowing an incident to continue, thereby increasing the damage and loss resulting from the unidentified and unreported malicious activity. During this phase of the incident life cycle, the incident handler or automated detection systems will review the incoming event data, identify what type of activity is occurring, and determine if an anomalous event shall be treated as a reportable cyber event or incident. Initial information to be reviewed will include, where available:

1. General description of the problem, event, or activity.
2. Status (ongoing or ended; successful or unsuccessful).
3. Number of ISs affected.
4. Source and destination Internet Protocol (IP) addresses.
5. Source and destination ports.
6. Hostname(s).
7. IS location.
8. User information.
9. Timestamps.
10. IDS alert and payload data (if relevant).

An event can be declared an incident at various points in the incident handling process, including during the preliminary analysis phase or the more detailed incident analysis phase. Sometimes, if an automated detection system is used, the criteria used to benchmark network traffic or IS activity may flag an event as an incident at the time it is detected.

### **3.2.1 Preliminary Analysis and Identification Methodology**

The following methodology will ensure a consistent approach to preliminary analysis and identification:



Figure - Preliminary Analysis and Identification Methodology

**Assess and Categorize**. Assess the event against the incident criteria to determine if it is a reportable cyber event or incident. Confirmed reportable events or incidents shall be categorized using Appendix A to Enclosure B (Cyber Incident and Reportable Cyber Event Categorization). In cases where more than one category applies, the category of highest precedence is used as outlined in the appendix. The security classification of the incident is determined at this stage in accordance with DoDI O-3600.02, “Information Operations (IO) Security Classification Guidance”, or local CC/S/A/FA original classification authority approved classification guidance. Based on the incident’s category, nature, and impact, determine if the computer forensics process should be initiated.

**Perform Preliminary Impact Assessment**. Determine the potential damage of the reportable cyber event or incident. This preliminary impact assessment should be conducted in accordance with [Appendix E, “Impact Assessment Matrix”](#_APPENDIX_E_–). The initial assessment shall be performed quickly, even with limited details and analysis. As the investigation continues and a more accurate characterization of the true impact is understood, the report is reassessed and modified. To make an accurate impact assessment, the analyst performing the preliminary assessment must have access to personnel with a good understanding of the function and criticality of the IS, information network, or data in question and its role in fulfilling the CC/S/A/FA mission (or ensure that those who do have that knowledge are informed).

**Begin or Continue Documentation**. Begin to document the incident if documentation has not already begun. If it has been determined that computer forensics are required (e.g., LE investigation), then begin to document the chain of custody. Documentation should include:

* 1. All known information about the cyber event or incident.
  2. All actions taken during the preliminary analysis activities and the results of that analysis.
  3. A chain of custody record initiation determination made by LE/CI if forensic evidence is collected and further prosecutorial investigation may be a consideration.

**Submit Initial Report**. Prepare and submit the initial report to the appropriate organizations and commands and through the appropriate reporting mechanisms. Incident reporting procedures identified in [Attachment B, “Cyber Incident Reporting”](#_APPENDIX_B_–) will be followed. Timelines for reporting are outlined in [Table 7, “Reporting Timelines”](#Table7). Additional guidance on reporting timeframes are provided by command authority OPORDs or other specific guidance. Incidents and reportable events shall be reported at the appropriate classification level using the appropriate means (i.e., Non-secure Internet Protocol Router Network (NIPRNET) e-mail or normal telephone for unclassified incidents and Secret Internet Protocol Router Network (SIPRNET) or secure telephone for Secret incidents). E-mails reporting an incident must be digitally signed at a minimum. Incident reporting will be conducted out of band from the involved network. Do not use assets on an information network that is (or potentially has been) compromised because an attacker may be monitoring the compromised network and could be warned of detection.

## **3.3 Preliminary Response Actions**

Preliminary response includes the coordinated and initial action(s) taken to protect the information network or IS from any further malicious activity and to acquire the data required for further analysis. Preliminary response actions are the immediate steps taken once an incident has been detected and declared. These actions are important as they provide information to help protect the ISs and information network from more damage while more detailed analysis is completed. More detailed response steps may be taken after a more thorough analysis is performed. These will be based on the nature, scope, and potential impact of the incident. The primary objectives of preliminary response include:

1. Preventing a reportable cyber event or incident from causing further damage.
2. Maintaining control of the affected IS(s) and the surrounding environment.
3. Ensuring forensically sound acquisition of data necessary
4. Maintaining and updating the incident report and actively communicating updates through the appropriate technical and operational command channels.

### **3.3.1 Preliminary Response Action Methodology**

The following methodology will ensure a consistent approach to preliminary response and action:



Figure - Preliminary Response Actions

**Contain the Incident**. Contain any potential threat to protect the affected IS or information network and prevent any further contamination, intrusion, or malicious activity. Containment can be done by an automated detection system or by incident handling staff working in conjunction with technical and management staff. Containment will be coordinated with the supporting CNDSP. The commander and supporting CNDSP will coordinate with LE/CI as required. Containment actions that may affect the ability to acquire and preserve data about the incident must be decided on carefully. When making these decisions, it is important to assess the relative value of ensuring mission success by preventing further damage against the potential for containment actions to hinder further analysis.

**Acquire and Preserve Data**. Safely acquire and preserve the integrity of all data (as directed) to allow for further incident analysis. All incidents require that as much data as possible be acquired and its integrity preserved. This includes volatile data (system registers, cache, and Random- Access Memory (RAM)), persistent data (system images, log files, and malware), and environmental data (environment, location, and configuration around the system). This data is necessary to support LE/CI investigations and to conduct incident analysis to fully understand the scope and impact of the incident. The IS will not be shut down or disconnected from the information network prior to acquiring and preserving the data (e.g., making a system image) unless authorized by the CNDSP or command authority. However, an exception to this requirement should be made if the machine begins to perform destructive tasks such as deleting files or formatting drives. In that case, the computer should be shut down quickly. Data from related systems or devices (e.g., routers, IDS/intrusion prevention system (IPS), domain controllers, and AV servers) that potentially aid in incident analysis will be acquired and preserved.

If an incident affects a large number of ISs, it may be impractical to acquire and preserve the data from each IS. An example would be an incident involving 100 user workstations containing no sensitive data that were compromised using the same delivery vector. In such cases, data must be acquired and preserved to the extent that the data provides new and/or additional information that could help in the technical analysis required to understand the nature, scope, and potential impact of the incident. Therefore, each IS may not require data acquisition and preservation (e.g., system images). However, prior to invoking this COA, the relevant CNDSP or command authority must approve that such data acquisition and preservation is not required.

Extenuating circumstances may prohibit the acquisition of data. For instance, there may be insufficient tools and/or resources. Alternatively, the acquisition may jeopardize mission-critical responsibilities or cause major operational mission degradation. In all cases, the CNDSP or command authority must approve that such data acquisition is not to be done.

**Continue Documentation**. Update the incident report with any actions taken during the preliminary response step and other useful information that may help to better characterize the incident. Any steps taken by first responders that potentially change the status or state of the affected IS must be documented. For example, actions such as taking the IS offline or touching any files on the IS will change the state of the information to be collected—including file access times, running processes, and memory contents. If this information is changed and not documented, it can potentially corrupt the admissibility of the forensic evidence collected in an investigation. For this reason, it is important to document any actions taken on the affected IS or service.

## **3.4 Incident Analysis**

Cyber incident analysis is a series of analytical steps taken to find out what happened in an incident. The purpose of this analysis is to understand the technical details, root cause(s), and potential impact of the incident. This understanding will help in determining what additional information to gather, coordinating information sharing with others, and developing a COA for response. The primary objectives of this phase include:

1. Ensuring the accuracy and completeness of incident reports.
2. Characterizing and communicating the potential impact of the incident.
3. Systematically capturing the methods used in the attack and the security controls that could prevent future occurrences.
4. Researching actions that can be taken to respond to and eradicate the risk and/or threat.
5. Understanding patterns of activity to characterize the threat and direct protective and defensive strategies.
6. Identifying the root cause(s) of the incident through technical analysis.

It is important to understand the different types of incident analysis. For most incidents, the CNDSP incident handlers will conduct (or coordinate) a system analysis to gather any necessary information from or about the affected IS(s). Depending on the type of incident (or reportable event) activity, if network or malware information is also available, then the CNDSP will also conduct (or coordinate) a network analysis and/or malware analysis, as appropriate. If there is a chance the incident might meet the criteria for reporting an incident to LE/CI for the purposes of pursuing a disciplinary, criminal, or CND investigation, then computer forensics evidence collection and analysis must be performed.

### **3.4.1 Incident Analysis Methodology**

The following methodology will ensure a consistent approach to incident analysis:



Figure - Incident Analysis Methodology

**Gather Information**. Identify and collect all relevant information about the incident for use in incident analysis. Information gathered may include data previously acquired and preserved, external logs, personal accounts, all-source intelligence, technical information, or the current operational situation. Any software artifacts suspected of being malware should be submitted to the Joint Malware Catalog (JMC).

**Validate the Incident**. Review, corroborate, and update (if applicable) the reported incident to ensure all information is accurate as reported. Reports should be reviewed and updated to maintain situational awareness, to add to incomplete information, or to correct erroneous information contained in the report. Report validation may require the review of trusted network and system logs or affected ISs to determine if the suspected activities happened as reported. Verify that the incident is categorized properly, in accordance with [Appendix A, “Cyber Incident and Reportable Event Categorization”](#_APPENDIX_A_–).

**Determine Delivery Vector(s)**. Analyze the information to determine the delivery vector(s) used by the threat actor. The delivery vector is the primary path or method used by the adversary to cause the incident or event to occur. Delivery vectors are used to systematically record major classes of delivery vectors used by adversaries. They do not identify the system specific root cause(s) of an incident. If more than one delivery vector is identified, distinguish between the primary and secondary delivery vectors used by the threat actor. For example, use of socially engineered e-mail delivering a malicious payload exploiting a known vulnerability that was preventable. Delivery vectors should be assessed in accordance with [Appendix D, “Delivery Vectors”](#_APPENDIX_D_–).

**Determine System Weaknesses**. Analyze the information to determine any underlying system weaknesses, vulnerabilities, or security controls that could have prevented or mitigated the impact of the incident. Identification of system weaknesses is a process used to systematically record and categorize major classes of security controls that could prevent similar incidents from occurring in the future. They cannot identify the system-specific root cause(s) of an incident.

**Identify Root Cause(s)**. Analyze the information to determine the system-specific cause(s) of the incident. Root cause identification expands upon the identified delivery vector(s) and system weaknesses by precisely identifying the sets of conditions allowing the incident to occur. For example, a delivery vector may identify an unpatched system. This is useful for correlation and trending but is insufficient in identifying the specific cause of the incident and preventing against future occurrences. Root cause identification would determine missing patches or system configurations that allowed the incident to occur. The root cause(s) of an incident should (unless not practical) be determined prior to the recovery and reconstitution of any system, unless otherwise approved by your command authority. The decision to restore a system without identifying the root cause(s) of an incident must be weighed carefully as it may leave the system vulnerable. For example, if the root cause of an incident stemmed from a missing patch in the baseline configuration, a system restoration using the same baseline configuration would leave the IS open to future compromise. A risk assumed by one is potentially a risk shared by many. Failing to identify the root cause of an incident may expose multiple commands and organizations to increased risk, especially in situations where they share similar configurations or defensive measures.

**Determine Impact**. Analyze the information gathered to validate and expand on the original impact assessment done during the preliminary analysis. Impact should be assessed in accordance with [Appendix E, “Impact Assessment Matrix”](#_APPENDIX_E_–). The impacts to be determined are as follows:

1. Technical Impact (TI). TI refers to an incident’s detrimental impact on the technical capabilities of the organization. TI typically refers to impacts on the information network or IS machines directly or indirectly affected by the incident.
2. Operational Impact (OI). OI refers to a detrimental impact on an organization’s ability to perform its mission. This may include direct and/or indirect effects that diminish or incapacitate IS or information network capabilities, the compromise and/or loss of DoD data, or the temporary or permanent loss of mission-critical applications or ISs.

**Research and Develop COAs**. Identify actions necessary to respond to the reportable cyber event or incident, fix the IS, and assess the risk for the IS or information network. Analysis, comparison, and selection of the best COA could be done at the lowest command possible. For instance, a commander could be the approving authority for an incident response COA for his or her base. USSTRATCOM, through USCYBERCOM, reserves the right to redirect all response actions for incidents that fall into a DoD Enterprise Incident Set. In some cases, in coordination with the Tier II CNDSP, AO (DAA), and USSTRATCOM, the commander may decide to leave the IS vulnerable and accessible in order to monitor the attacker’s activities. This may be done to assist an LE/CI investigation or for network defense and operational purposes. COA may include CND Response Actions (CND RAs) as outlined in CJCSI 3121.01, “Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces.” Actions that potentially affect traffic on the DoD Protected Traffic List must be coordinated with USCYBERCOM.

**Coordinate with Others**. Work with other appropriate parties to collect additional information, obtain assistance and additional expertise or guidance, and notify appropriate operational and technical channels regarding changes in the status of reportable events, incidents, and incident handling activities. Timely interagency coordination and de-confliction of operations are crucial to conducting an effective incident response. For additional guidance, refer to [Appendix F, “Coordination and De-confliction”](#_APPENDIX_F_–). Coordination ensures that the identification and de-confliction of response is vetted through all the parties that may be affected by the response.

Coordination may include the following:

1. Reporting vertically to alert higher HQ and other CND organizations.
2. Reporting horizontally to other peer organizations that have ISs that may be affected.
3. Researching and planning response strategy and COA

**Perform Correlation and Trending**. This involves analyzing and identifying relationships and trends between incidents in the short term and patterns across incidents in the long term. Effective and complete reporting throughout the incident handling life cycle ensures that the Department of Defense has the ability to conduct and identify these trends and patterns. Trending analysis involves understanding and accurately characterizing the relationship of incidents reported and providing awareness of the cyber security trends as observed by the affected parties. It includes analysis based on incident information that has been reported to the constituent, incidents identified by the constituent, and public/private sector information identified when correlating and analyzing the data.

## **3.5 Response and Recovery**

Response and recovery include the detailed response steps performed to prevent further damage, restore the integrity of affected ISs, and implement follow-up strategies to prevent the incident from happening again. The primary objectives for performing response and recovery include:

1. Resolving the incident according to policy, procedures, and quality requirements.
2. Mitigating the risk or threat.
3. Restoring the integrity of the IS and returning it to an operational state.
4. Implementing proactive and reactive defensive and protective measures to prevent similar incidents from occurring in the future.
5. Completing a battlefield damage assessment (BDA) IAW [Appendix E, “Impact Assessment Matrix”](#_APPENDIX_E_–).

Response and recovery may require a combination of technical, management, and/or LE/CI actions. Technical actions include changes in the network and IS infrastructure to remove the risk or threat. Management steps can include administrative, human resources, public relations, or policy creation and management activities. LE/CI actions can include further investigation or criminal prosecution. Other management issues may involve legal actions to handle liability, service level agreements, or contracting issues.

### **3.5.1 Response and Recovery Methodology**

The following methodology will ensure a consistent approach response and recovery:



Figure - Response and Recovery Methodology

**Implement Containment**. Implement (if applicable) additional containment actions to regain control of or isolate the system and prevent further malicious activity. Determine the appropriate containment strategy based on the type of incident. Examples of strategies might include modifying network access controls (e.g., firewalls), installing new AV or IDS/IPS signatures, or making physical changes to the infrastructure. Collaborate with partners since investigative or intelligence equities may need to be considered before certain containment measures are taken. See Enclosure F for a full discussion of collaboration.

**Eradicate Risk**. Eradicate the risk and take actions that remove the cause of the incident from the IS/network. No system should be rebuilt until system data has been adequately preserved and the vulnerability has been mitigated. ISs having a Category (CAT) 1, 2, and 7 cyber incidents must be rebuilt from trusted media and have up-to-date AV software loaded and configured IAW Security Technical Implementation Guides (STIGs) and warning and tactical directives/orders (e.g., WARNORDs, FRAGOs, TASKORDs, etc.) prior to connecting the IS to the information network. Mission impact may require patching the affected component and instituting temporary vulnerability mitigation until the mission allows the IS to be rebuilt.

**Recover from Incident**. Fully restore affected data and ISs to normal operation (if applicable). Harden ISs to prevent similar incidents and monitor them to ensure the IS is completely free from the original IS weakness. For some incidents, eradication is either not necessary or is performed during recovery. Preventing similar incidents may involve changing baseline configurations, tightening network perimeter security, updating AV and scanning tool signature files, rebuilding the system from trusted media, conducting user training, or implementing countermeasures that mitigate the risk.

**Coordinate with Others**. Work with appropriate parties to implement COAs and resolve cyber events or incidents.

**Notify Others**. Notify any relevant stakeholders or participants of actions they need to take. Notify involved parties (as appropriate) of the status of the incident and progress of the response. Submit updated information on the incident and the progress of the response to keep higher CND organizations and/or HQ updated on the status of the incident response. CC/S/A/FAs must ensure that program managers for centrally managed programs are notified of CAT 1, 2, 4, 5, or 7 cyber incidents impacting their programs (Appendix A to Enclosure B).

**Continue Documentation**. Update the incident record in JIMS with information on any response and recovery steps that were taken. Each update to the JIMS report provides a more complete understanding of the incident. Consistent and frequent updates provide a platform to broadly characterize adversarial activity and enable USCYBERCOM to direct appropriate defensive actions for all DoD information networks.

**Update Response Actions and Battlefield Damage Assessment (BDA) and Close Incident**. Update the incident record in JIMS that closes out the incident. Ensure all parties have completed the necessary actions for the response. The BDA documents the technical and operational impact (i.e.,OPSEC assessment) of the incident on the organization. It should be determined IAW [Appendix E, “Impact Assessment Matrix”](#_APPENDIX_E_–). Update the JIMS incident record with the BDA within 24 hours after the incident is resolved. Declare the incident closed, change the status in the JIMS to closed, and perform any other actions to close the incident. Incidents cannot be closed as a CAT 8—Investigating. An incident might be closed for the CC/S/A/FA or the CNDSP but still remain open for LE/CI investigation. **CNDSPs are responsible for closing an incident.** Incidents may be reopened by USCYBERCOM if necessary, in which case the affected CNDSP would be contacted and given direction as to what additional actions should be taken.

## **3.6 Post-Incident Analysis**

Post-incident analysis involves a postmortem on an incident to review the effectiveness and efficiency of incident handling. Data captured in the postmortem includes lessons learned, initial root cause, problems with executing COAs, missing policies and procedures, and inadequate infrastructure defenses. Postmortem results should be used to improve the incident management process and methodology and the security posture and defenses of the CC/S/A/FAs.

One of the most important parts of incident handling is learning how to improve operations, processes, and infrastructure defenses by reviewing how an incident happened and how the response was handled. The primary objectives for post-incident analysis include:

1. Identifying infrastructure problems to address.
2. Identifying organizational policy and procedural problems to be addressed.
3. Identifying technical or operational training needs.
4. Determining unclear or undefined roles, responsibilities, interfaces, and authority.
5. Improving tools required to perform protection, detection, analysis, or response actions.

Not all incidents require a postmortem. Usually, incidents that are large in scope, handled poorly, involved LE, or caused severe damage require a postmortem. Incidents that do require a postmortem will be sent to USCYBERCOM.

# **4.0 INFORMATION SPILLS**

Classified (or sensitive) data spills occur when classified data is introduced onto an unclassified information system, to an information system with a lower level of classification, or to a system not accredited to process data of that restrictive category. Although it is possible that no actual unauthorized disclosure occurred, classified data spills are considered and handled as a possible compromise of classified information involving information systems, networks and computer equipment until the inquiry determines whether an unauthorized disclosure did or did not occur.

The following personnel are responsible for responding to information spills:

|  |  |  |  |
| --- | --- | --- | --- |
| Title | Name | Email | Phone Number |
| ISSM | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| ISSO | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |

The process for responding to information spills is contained within DODM NUMBER 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information" and local policies. Guidance requires After Actions Report (AAR) creation to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

# **APPENDIX A – CYBER INCIDENT AND REPORTABLE CYBER EVENT CATEGORIZATION**

A Cyber Incident or Reportable Cyber Event Category is a collection of events or incidents sharing a common underlying cause for which an incident or event is reported. Each cyber event or incident is associated with one or more categories as part of the incident handling process. In cases where more than one category applies, the category assigned should be determined using the following precedence. The following table describes the category precedence for incidents.

|  |  |  |
| --- | --- | --- |
| Precedence | Category | Description |
| 0 | 0 | Training and Exercises |
| 1 | 1 | Root Level Intrusion (Incident) |
| 2 | 2 | User Level Intrusion (Incident) |
| 3 | 4 | Denial of Service (Incident) |
| 4 | 7 | Malicious Logic (Incident) |
| 5 | 3 | Unsuccessful Activity Attempt (Event) |
| 6 | 5 | Non-Compliance Activity (Event) |
| 7 | 6 | Reconnaissance (Event) |
| 8 | 8 | Investigating (Event) |
| 9 | 9 | Explained Anomaly (Event) |

Table - Category Precedence

Investigating (Category 8) reports will include an initial assessed incident category (Categories 1-7 or 9) and be re-categorized based on continued investigation. No reports will be closed as a Category 8. The following table provides incident and reportable event categories.

| Category | Description |
| --- | --- |
| 0 | **Training and Exercises**—Operations performed for training purposes and support to CC/S/A/FA exercises. |
| 1 | **Root Level Intrusion (Incident)**—Unauthorized privileged access to an IS. Privileged access, often referred to as administrative or root access, provides unrestricted access to the IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category. |
| 2 | **User Level Intrusion (Incident)**—Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user level access, provides restricted access to the IS based on the  privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category. |
| 3 | **Unsuccessful Activity Attempt (Event)**—Deliberate attempts to gain unauthorized access to an IS that are defeated by normal defensive mechanisms. Attacker fails to gain access to the IS (i.e., attacker attempts valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders.  Note the above CAT 3 explanation does not cover the “run-of-the- mill” virus that isdefeated/deleted by AV software. “Run-of-the- mill” viruses that are defeated/deleted by AV software are not reportable events or incidents and should not be annotated in JIMS. |
| 4 | **Denial of Service (Incident)**—Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information network. |
| 5 | **Non-Compliance Activity (Event)**—Activity that potentially exposes ISs to increased risk as a result of the action or inaction of authorized users. This includes administrative and user actions such as failure to apply security patches, connections across security domains, installation of vulnerable applications, and other breaches of existing DoD policy. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders. |
| 6 | **Reconnaissance (Event)**—Activity that seeks to gather information used to characterize ISs, applications, DoD information networks, and users that may be useful in formulating an attack. This includes activity such as mapping DoD information networks, IS devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise. |
| 7 | **Malicious Logic (Incident)**—Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This **only** includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Category 1 or Category 2 incidents, not Category 7. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS. |
| 8 | **Investigating (Event)**—Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review. No event will be closed out as a Category 8. Category 8 will be re-categorized to appropriate Category 1-7 or 9 prior to closure. |
| 9 | **Explained Anomaly (Event)**—Suspicious events that after further investigation are determined to be non-malicious activity and do not fit the criteria for any other categories. This includes events such as IS malfunctions and false alarms. When reporting these events, the reason for which it cannot be otherwise categorized must be clearly specified. |

Table - Cyber Incident and Reportable Cyber Event Categories

# **APPENDIX B – CYBER INCIDENT REPORTING**

Incident reporting comprises a well-defined framework for the timely reporting of any reportable cyber event or incident. It ensures the report provides an accurate, meaningful, and complete understanding of the incident, from initial detection through analysis to resolution and closure. This section provides guidance on the reporting requirements for reportable cyber events and incidents. There are two primary reporting structures, which are described below.

1. Technical Reporting Structure. This structure consists primarily of global USCYBERCOM (Tier I), regional/theater/CC/S/A/FAs (Tier II) CNDSPs, and local (Tier III) organizations and describes the interactions between each of the tier levels and how reporting, notification, and communications shall occur.
2. Additional Reporting Structures. This group includes other reporting structures that may be required in support of the IC, LE/CI, and operational and any other external organizations as appropriate.

The following table summarizes reporting vehicles available in order of preference. Other mechanisms should only be used when the JIMS cannot be accessed or when circumstances require the use of other reporting channels. Regardless of how initial reporting is done, information regarding the report must be added to the JIMS:

|  |  |
| --- | --- |
| Order | Method |
| Data | |
| 1 | Joint Incident Management System (JIMS) - SIPRNet |
| 2 | Defense Message system (DMS) – SIPRNet (record message traffic) |
| 3 | E-Mail SIPRNet |
| 4 | NIPRNet with security protection (e.g. digital signature and encryption). Last resort used for only initial information |
| 5 | NIPRNet without security protection (e.g. no encryption). Last resort used for only initial information |
| Fax/Voice | |
| 1 | Secure fax |
| 2 | Secure Telephone Equipment (STE) |
| 3 | Defense Red Switch Network (DRSN) |
| 4 | Non-Secure fax. Last resort used for only initial information |
| 5 | Defense Switched Network (DSN). Last resort used for only initial information |

Table - Incident Report Vehicles

Technical Reporting is designed to assist with the handling of incidents and provide fixes to mitigate the operational and/or technical impact of an incident.

**Tier I Reporting**. Tier I receives reports from Tier II and external entities. It is positioned for centralized coordination and control in a way that allows it to broadly characterize attacks occurring across the Department of Defense. This vantage point allows it to provide tactical and strategic direction to subordinate levels and determine defensive and/or protective strategies that help improve the overall security posture of the DoD Information Networks. Tier I includes USCYBERCOM and supporting entities

**Tier II Reporting**. Tier II receives reports from the subordinate levels (Tier III). This information can also be shared (if applicable) with other Tier II entities to provide insight into activity that can potentially affect its region or theater of operations. Tier II organizations report incidents to USCYBERCOM. All incident reports should be submitted through the JIMS unless prevented by extenuating circumstances (e.g., no access to JIMS). All organizations must report through their CNDSP. The CNDSP enters the report into the JIMS. Lateral reporting may be required by their operational or administrative chain of command.

**Tier III Reporting**. Tier III initiates local operational reporting and receives support from and responds to direction from a designated Tier II CNDSP. Tier III reporting, notification, and communication provides information about what is occurring to the Network Service Centers (NSCs) at Service component headquarters, major commands, and Service elements at installations (e.g., base, post, camp, and station (B/P/C/S) information systems or joint activities that serve as a focal point for reporting and handling incidents and network management at the lowest level).

Additional Reporting Structures is designed to assist with the handling of incidents and provide fixes to mitigate the operational and/or technical impact of an incident.

**Operational Report (OPREPs)**. OPREPs are issued by any unit commander to provide appropriate senior leadership immediate notification of an incident that has impacted or may impact the mission and/or operations. Specifically, Category 1, 2, 4, and 7 events or incidents affecting Mission Assurance Category (MAC) I or II ISs must be reported using OPREP-3 reporting procedures and structure. OPREP-3 reports will be submitted as soon as possible after cyber incidents have been detected. Speed takes priority over detail. USCYBERCOM submits OPREP-3 for DoD-wide computer network incidents to USSTRATCOM.

**Law Enforcement and Counterintelligence Reporting Structure**. CND reportable events or incidents that may lead to criminal investigations require notification and reporting to LE/CI. Data from the incident will be preserved in a forensically sound manner to enable possible criminal prosecution or LE/CI operations. At minimum, Category 1, 2, and 4 incidents are reported to DoD LE/CI IAW established CC/S/A/FA procedures. Incidents involving potential or actual compromise of classified ISs or DoD information networks are reported through standard CND technical reporting channels. Commanders request investigations and the servicing LE/CI organization determines if investigations are to be opened IAW DoDI 5505.3. Incidents are reported to the appropriate LE/CI organization at the lowest level at which they are discovered IAW established CC/S/A/FA procedures. Reporting incidents through LE/CI channels does not eliminate the requirement to report incidents through standard technical and operational reporting channels.

**Intelligence Community Reporting Structure**. IC reporting is required for any reportable events or incidents that affect classified ISs or involve foreign threats to DoD information networks and ISs. CC/S/A/FAs report incidents (or reportable events) affecting Top Secret (TS)/SCI networks directly to organizations as directed under SCI directives and policies as provided by the principal accrediting authority. DoD SCI organizations will provide reporting directly to the DIA Information Assurance Protection Center (IAPC). Member organizations operating under the authority of the NSA, NRO, and NGA shall report to their agency authority IAW internal agency policy. DoD IC members will report all reportable events directly to the IC-IRC within established reporting timelines.

The reporting timelines establish the minimum requirements and timeframes by which incidents will be reported. USCYBERCOM may issue changes to reporting requirements and timeframes based on ongoing operations or activities. The reporting timelines are designed to expedite reporting of incidents where national-level coordination and action may serve to mitigate or prevent damage to the DoD information networks.

| Category | Impact | Initial Notification to Next Tier | Initial Report to Next Tier | Initial submission to JIMS | Minimum Reporting |
| --- | --- | --- | --- | --- | --- |
| 1- Root Level Intrusion (Incident) | High | Within 15 minutes | Within 4 hours | Within 6 hours | Tier I |
| Moderate | Within 2 hours | Within 8 hours | Within 12 hours | Tier I |
| Low | Within 4 hours | Within 12 hours | Within 24 hours | Tier I |
| 2- User Level Intrusion (Incident) | High | Within 15 minutes | Within 4 hours | Within 6 hours | Tier I |
| Moderate | Within 2 hours | Within 8 hours | Within 12 hours | Tier I |
| Low | Within 4 hours | Within 12 hours | Within 24 hours | Tier I |
| 3- Unsuccessful Activity Attempt (Event) | Any | Within 4 hours | Within 12 hours | Within 24 hours | Tier II |
| 4- Denial of Service (Incident) | High | Within 15 minutes | Within 4 hours | Within 6 hours | Tier I |
| Moderate | Within 15 minutes | Within 4 hours | Within 6 hours of discovery | Tier I |
| Low | As directed by CC/S/A/FA Guidance | As directed by CC/S/A/FA Guidance | As directed by CC/S/A/FA Guidance | Tier I |
| 5- Non- Compliance Activity (Event) | All Noncompliance Events | Within 4 hours | Within 12 hours | Within 48 hours | Tier II |
| 6 – Reconnaissance (Event) | Any | As directed by CC/S/A/FA Guidance | As directed by CC/S/A/FA Guidance | As directed by CC/S/A/FA Guidance | Tier II |
| 7 - Malicious Logic (Incident) | High | Within 15 minutes | Within 4 hours | Within 6 hours | Tier I |
| Moderate | Within 2 hours | Within 8 hours | Within 12 hours | Tier II |
| Low | As directed by CC/S/A/FA Guidance | As directed by CC/S/A/FA Guidance | As directed by CC/S/A/FA Guidance | Tier II |
| 8 - Investigating (Event) | N/A | Within 2 hours of notification[6](#_bookmark5) | Consistent with the most severe possible interpretation | Within 24 hours | Tier II |
| 9 - Explained Anomaly (Event) | N/A | N/A | Within 24 hours | Within 72 hours | Tier II |

Table - Incident Reporting Timelines

# **APPENDIX C – GENERAL CYBER INCIDENT REPORT FORMAT**

The following table describes the report format used for the initial report of an incident or reportable event. The format provides a structure for reporting initial incidents by secure fax, telephonically, or by other electronic means. Initial reports may be incomplete. Reporting organizations should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.

| Field | Description |
| --- | --- |
| Cyber Incident Tracking Information | |
| Reporting Incident Number | Identify the reporting CNDSP (e.g., CERT/CIRT) reference number for tracking the incident. (Generated by JIMS.) |
| Organization Tracking | Identify the organization responsible for tracking the incident. |
| Reporting Information | |
| Name | The first and last name of the individual reporting the incident. |
| Organization | The name of the organization reporting the incident. |
| Telephone | The telephone or Defense Switch Network (DSN) number to be used to reach the reporting entity for additional information. The number can be for an individual’s number or the central number for the organization (e.g., operations center). |
| E-mail | The e-mail address that should be used to reach the reporting entity for additional information. This may be the e-mail address of an individual or central e-mail for the organization (e.g., operations center). |
| Fax | The fax number to be used to reach the reporting entity for additional information. |
| Alternative Contact | The name, telephone number, and e-mail of an alternative contact in the event the reporter is not available. |
| Categorization Information | |
| Primary Incident Category | Identify the primary underlying cause of the incident being reported IAW Appendix A to Enclosure B (Incident and Reportable Event Categorization). |
| Secondary Incident Category | Identify any secondary causes for which the incident is being reported, if more than one category applies, IAW Appendix A to Enclosure B (Incident and Reportable Event Categorization). |
| Delivery Vector | Identify delivery vector IAW Appendix A to Enclosure D (Delivery Vectors.) |
| System Weaknesses | Identify delivery vector IAW with Appendix B to Enclosure D (System Weaknesses). |
| Incident Status | |
| Status | Status of the incident (“OPEN,” “INVESTIGATING,” “MITIGATED,” or “CLOSED”). |
| Incident Start Date | ZULU date-time group (DTG) of the earliest event that was incorporated into the incident. Provide year/month/day/hour/minute/ seconds. |
| Incident End Date | ZULU DTG that incident actually ended. Provide year/month/day/hour/ minute/seconds. |
| Last Update | ZULU DTG of the last time the report was updated. Provide year/month/day/hour/minute/seconds. |
| Date Reported | ZULU DTG of when the incident was first reported to the CNDSP. Provide year/month/day/hour/minute/seconds. |
| System Classification | Report the classification of the IS under attack (i.e., Unclassified, Confidential, Secret, TS, SCI). This field is NOT used to classify the reported incident. |
| Action Taken | Indicates what action has been taken in response to the incident. Include notifications and associated reports. Additionally, include whether a copy of a media was taken (image hard drives), or logs collected and |
| Technical Details | |
| Event/Incident Description | Provide a narrative description of the incident with technical details. Include DTGs of significant events (start, stop, or change of activity). State the use of the targeted IS and whether the IS is online or offline. Indicate whether the incident is ongoing. |
| Root Cause(s) | Identify the IS specific cause(s) of the incident. The root cause expands upon the identified delivery vector(s) and IS weaknesses by precisely identifying the sets of conditions allowing the incident to occur. Indicate whether the DAA or CIO had accepted a risk that led to the incident. |
| Source IP and Port | Provide source IP with resolution data identifying owner and country of source IP machine. Note: The source IP could be a DoD IP. If the intruder is known, provide all identifying information to include the intruder’s objective, if known. Source IP is not necessarily indicative of true origin. Footnote the source of resolution/attribution data (i.e., ARIN.org). Insert “Not Applicable” for incidents that do not involve source IP or port. |
| Intruder(s) (if known) | Identify the intruder or group responsible for the incident, if known. |
| Origin (Country) | Identify the source IP’s country of origin. |
| Target IP(s) and Port | Provide target IP with resolution identifying responsible command and physical location of target IP machine (e.g., B/C/P/S, etc.). Footnote the source of resolution/attribution data (i.e., DDD NIC, nslookup, and whois). If machine is behind a network address translation enabled (NAT’ed) router or firewall then also provide the wide area network (WAN) routable address (i.e., the Internet/SIPRNET routable IP address). |
| Technique, Tool, or Exploit Used | Identify the technique, tool, or exploit used. |
| Operating System (OS) and OS Version | Record the OS and version number of the OS where the incident occurred. |
| Use of Target (e.g., Web Server, File Server, Host) | What the intruder/attacker used the target IS for, after it was exploited, if applicable. |
| Method of Detection | Identify how the intrusion was detected (e.g., external notification, log files, network monitoring, IDS, user). |
| Sites Involved | |
| Major Command | Identify the CC/S/A/FAs targeted based on owner of target IP address (e.g., USN, USAF, USSTRATCOM, and DISA). |
| Combatant Command | Identify the Combatant Command (geographical and/or functional) targeted based on the owner of the target IP address. |
| Physical Location (base, camp, post, or station) | Identify the B/C/P/S affected by the intrusion and/or who owns the target IP and where the physical system resides. |
| DoD Information Network | Identify the DoD information network on which the incident occurred (e.g., NIPRNET or SIPRNET). |
| Detecting Unit or Organization | The name of the reporting unit or organization. |
| Affected Unit or Organization | The name of the reporting affected unit or organization. |
| Impact Assessment | |
| Systems Affected | Number of ISs affected by the incident. |
| Operational Impact | Identify any detrimental effects on ability to perform mission by organization directly affected. Include organizations affected (e.g., due to being network users). Include impact on the ability of other organization(s) to perform mission. This includes an operational impact assessment IAW Appendix C to Enclosure D (Impact Assessment Matrix). |
| Technical Impact | Identify any detrimental effects on the technical capabilities of the organization (e.g., data loss, service degradation, effects on other systems). This includes a technical impact assessment IAW Appendix C to Enclosure D (Impact Assessment Matrix). If the technical impact cannot be determined for some reason (e.g., limited details or analysis), use Table C-B-2 (Initial Impact Assessment) for a limited impact assessment. |
| Staff Hours Lost | This is reported as an update record and may cause the impact field to be updated. Amount of time technical support is required to identify, isolate, mitigate, resolve, and recover from the attack and repair the attacked IS (do not include analyst time spent analyzing the incident). |
| Encompassing Cost | Costs (both direct and indirect), to include all actions from initial detection through investigation, response, and recovery. This should include, but is not limited to, workforce expenses, analyst time, hardware / software, travel and shipping costs, and lost productivity. |
| Additional Reporting or Coordination | |
| OPREP 3 Reporting | State whether the incident was reported via OPREP 3 and what HQ received the report. Attach a copy of the OPREP 3 report to this incident report, if applicable. |
| Intel Reporting | State whether the incident was reported to the IC. If reported, identify the agency contacted and any specific actions that have been coordinated. |
| LE/CI Reporting | State whether the incident was reported to the LE/CI community. If reported, identify the agency contacted and any specific actions that have been coordinated. |
| DAA/CIO Reporting | Notify and coordinate with the DAA/CIO on cyber incidents. |
| Other | |
| Exercise Name | Name of the exercise, if applicable. |
| Operation Name | Name of the operation or focused operation, if applicable. |

Table - Report Format

# **APPENDIX D – DELIVERY VECTORS**

A delivery vector is defined as the primary path or method used by the adversary to cause the incident or event to occur. This information is collected as part of the incident report and used to identify trends in the prevalence of various vectors. By understanding the most prevalent vectors, tactical and strategic plans can be developed to improve the defensive posture of DoD information networks. Including the types of delivery vectors in the incident reporting can help USCYBERCOM correlate information across CC/S/A/FAs to identify potential Enterprise Incident Sets. Delivery vectors are very dynamic but can generally be grouped into several distinct categories. Sub-categories are more specific vectors and may be more dynamic (and therefore require changes over time).

The following table describes the major categories and sub-categories of delivery vectors. It should be used for assigning delivery vectors to reportable events or incidents. Given the complexity of some attacks, it is not uncommon for more than one delivery vector to be used in an attack. Therefore, a cyber event or incident may be assigned more than one delivery vector.

| Delivery Vector  Category Number | | Description |
| --- | --- | --- |
| 2 | Sub-category | **Authorized User**: A user with authorized access took specific actions that resulted in jeopardizing ISs or data. |
| A | Purposeful: An authorized user knowingly took specific actions that jeopardized ISs or data. |
| B | Accidental: An authorized user took actions that had consequences over and above the intentions and jeopardized ISs or data. |
| 3 | Sub-category | **Social Engineering**: Human interaction (social skills) or deception used to gain access to resources or information. |
| A | E-mail: E-mail is the primary vehicle used to deliver a malicious payload or gain access to resources or information. |
| B | Web site: A Web site is the primary vehicle used to deliver a malicious payload or gain access to resources or information. |
| C | Other: A user was deceived or manipulated in a way that is not covered by the other types of social engineering. |
| 4 | Sub-category | **Configuration Management**: Compromise resulting from the inadequate or improper configuration of an IS. |
| A | Network: An IS that provides network-based services was improperly or inadequately configured. |
| B | OS: An OS was improperly or inadequately configured. |
| C | Application: An application was improperly or inadequately configured. |
| 5 | Sub-category | **Software Flaw**: A vulnerability in the software that allows for the unauthorized use of or access to an IS in a way that violates the IS’s security policy. |
| A | Exploited New Vulnerability: This vulnerability was unknown prior to the event or there was no mechanism available to prevent it. |
| B | Exploited Known Vulnerability: This vulnerability was known prior to the event and there was a mechanism available to prevent it. |
| 6 | Sub-category | **Transitive Trust**: Compromise resulting from the implicit or explicit trust relationship between security domains. |
| A | Other IS Compromise: Compromise resulting from access previously gained on another IS. |
| B | Masquerading: Compromise resulting from the unauthorized use of a valid user’s credentials. This may include cryptographic material, account credentials, or other identification information. |
| 7 | Sub-category | **Resource Exhaustion**: The consumption of IS resources that prevents legitimate users from accessing a resource, service, or information. |
| A | Non-Distributed Network Activity: Activity from a single IP address that overwhelms IS or information network resources. This is generally associated with a DoS incident. |
| B | Distributed Network Activity: Activity from multiple IP addresses that overwhelms IS or information network resources. This is generally associated with a DoS incident. |
| 8 | Sub-category | **Physical Access**: The unauthorized physical access to resources. |
| A | Mishandled or lost resource: Equipment was stolen, lost, or left accessible to unauthorized parties. |
| B | Local access to IS: An unauthorized user was provided local physical access to a DoD information network resource. |
| C | Abuse of resources: The physical destruction of an information resource by an unauthorized party. |
| 9 | Sub-category | **Other** |
| A | New Delivery Vector: The delivery vector is not covered by the listed methods. Description of the delivery vector must be included in the incident comments. |
| 10 | Sub-category | **Unknown**. |
| A | Unable to Determine: Delivery vector could not be determined with the information available. |

Table - Delivery Vectors

The delivery vectors above are not exhaustive. Rather, they broadly define the major categories of delivery vectors. To provide a greater degree of granularity, a category may consist of subcategories that further characterize specific delivery vectors. For example, subcategories of the delivery vector “Software Flaw” may include “Exploited a New Vulnerability” or “Exploited an Existing Vulnerability.” This provides a greater degree of control over the type of information being reported.

# **APPENDIX E – IMPACT ASSESSMENT MATRIX**

Impact is assessed based on the degree to which an incident or event adversely affects, or has the potential to affect, the successful accomplishment of operational missions and the confidentiality, integrity, or availability of DoD information networks and ISs. Each cyber event or incident is assessed and assigned an impact as part of the incident handling process. An impact assessment is one of the determining factors when assigning priority to an incident or event. The category and impact guide reporting timelines and response actions should be commensurate with the magnitude of the incident or event.

The following table describes the categorization system for assigning impact levels to incidents or events. This table is intended to provide a high-level overview of each security objective and define impact levels across these objectives.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Potential Impact | | |
| Security Objective | **Low** | **Moderate** | **High** |
| Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44  U.S.C. 3542]. | The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| Integrity. Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. [44 U.S.C. 3542]. | The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| Availability. Ensuring timely and reliable access to and use of information. [44 | The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

Table - Impact Levels

# **APPENDIX F – COORDINATION AND DE-CONFLICTION**

Coordination and de-confliction ensure that incident response COAs are coordinated with all parties potentially affected by the response and in a way that prevents any unnecessary interference or overlap between ongoing activities. These actions must be vetted through all parties potentially affected by the response. For the purpose of this guidance, coordination and de-confliction are defined below:

1. Coordination is the act of exchanging information between organizations to provide situational awareness, collaboration on assessments, and synchronized response actions.
2. De-confliction is a subset of coordination in which information is shared to eliminate overlap or interference between ongoing activities.

Time-sensitive operations generally involve network-centric COAs to defend the DoD information networks against imminent or ongoing threats. Time-sensitive operations require coordination inputs from DoD and non-DoD organizations, with the timeliness required based on the threat and the operational situation as determined in the CCIR. As a general rule, inputs for time-sensitive operations will be required from all organizations within 4 hours of notification by USCYBERCOM. USCYBERCOM J2 will manage requests for IC coordination and de-confliction with the appropriate IC members. The LE/CI organizations (at USCYBERCOM) shall conduct LE/CI coordination and de-confliction with appropriate LE/CI organizations. (4) Organizations participating in the coordination and/or de-confliction process will provide POCs capable of responding 24 hours a day to take appropriate action or be able to recall necessary personnel who can complete the actions required within the required timeline.

Non-time-sensitive operations are network-centric and non-network-centric COAs to defeat or mitigate ongoing threats such as a persistent, sophisticated intruder. While coordination and de-confliction are important and all inputs will be considered by USCYBERCOM when deciding to approve or disapprove a particular course of action, non-concurrence from an organization does not constitute a veto over the operation. Non-time-sensitive coordination and de-confliction will use a more deliberative process employing periodic coordination and/or de-confliction meetings, correspondence, teleconferences, and video teleconferences. Non-time-sensitive coordination and de-confliction procedures shall be used when USCYBERCOM contemplates non-network-centric COAs, such as diplomatic initiatives, public affairs campaigns, law enforcement informational exchanges with foreign countries, etc., or when network-centric Tier I incident responses are necessary but not assessed as time sensitive. Coordination and/or de-confliction meetings will be held periodically (e.g., weekly, biweekly) with the IC, appropriate DoD LE/CI organizations, the LE/CI organizations, Combatant Commands, Service components, USCYBERCOM staff, and other government CND organizations as required.

For Insider Threats, LE/CI authorities and capabilities are typically the best option for addressing suspected and/or known access violations, theft, and damage caused by trusted insiders. Given that “insiders” represent a large population (e.g., U.S. military, government service civilians, contractors, and foreign national coalition partners), reports related to potential insiders will always be handled very cautiously. Coordination and de-confliction must occur across tiers, between agencies, and with other DoD or external organizations, as appropriate.

# **APPENDIX G – LESSONS LEARNED / AFTER ACTION REPORTS**

# **G.1.0 LESSONS LEARNED**

One of the most important parts of incident response is also the most often omitted: learning and improving. The {ACRONYM} incident response team will evolve to reflect new threats, improved technology, and lessons learned. Holding a “lessons learned” meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident. Questions to be answered in the meeting include:

1. Exactly what happened, and at what times?
2. How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
3. What information was needed sooner?
4. Were any steps or actions taken that might have inhibited the recovery?
5. What would the staff and management do differently the next time a similar incident occurs?
6. How could information sharing with other organizations have been improved?
7. What corrective actions can prevent similar incidents in the future?
8. What precursors or indicators should be watched for in the future to detect similar incidents?
9. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Small incidents need limited post-incident analysis, with the exception of incidents performed through new attack methods that are of widespread concern and interest. After serious attacks have occurred, it is usually worthwhile to hold post-mortem meetings that cross team and organizational boundaries to provide a mechanism for information sharing. The primary consideration in holding such meetings is ensuring that the right people are involved. Not only is it important to invite people who have been involved in the incident that is being analyzed, but also it is wise to consider who should be invited for the purpose of facilitating future cooperation.

The success of such meetings also depends on the agenda. Collecting input about expectations and needs (including suggested topics to cover) from participants before the meeting increases the likelihood that the participants’ needs will be met. In addition, establishing rules of order before or during the start of a meeting can minimize confusion and discord. Having one or more moderators who are skilled in group facilitation can yield a high payoff. Finally, it is also important to document the major points of agreement and action items and to communicate them to parties who could not attend the meeting.

Because of the changing nature of information technology and changes in personnel, the incident response team will review all related documentation and procedures for handling incidents at designated intervals.

# **G.2.0 AFTER ACTIONS REPORTS**

The After Actions Report (AAR) provides evaluation criteria based on the exercise objectives and a means to evaluate how well exercise objectives were met, and identify areas where additional exercises might be necessary. Evaluating the exercise is a critical step to ensuring success of the incident response program. After the test or exercise is complete, the participants will conduct a debriefing to discuss observations for things that worked well and things that could be improved. The comments that surface during the debriefing, along with lessons learned documented during the exercise, will be captured in the AAR. The AAR will also document observations made throughout the exercise and participants during the exercise and recommendations for enhancing the IR plan that was exercised.

The template used to document the AAR can be found in [Enclosure 1, “After Actions Report Template”](#_Enclosure_1_–).

# **G.3.0 METRICS**

The {ACRONYM} incident response team will collect the below data, which will be used to measure the success of the incident response team:

| Data | Description |
| --- | --- |
| Number of incidents Handled | Handling more incidents is not necessarily better—for example, the number of incidents handled may decrease because of better network and host security controls, not because of negligence by the incident response team. The number of incidents handled is best taken as a measure of the relative amount of work that the incident response team had to perform, not as a measure of the quality of the team, unless it is considered in the context of other measures that collectively give an indication of work quality. It is more effective to produce separate incident counts for each incident category. Subcategories also can be used to provide more information. For example, a growing number of incidents performed by insiders could prompt stronger policy provisions concerning background investigations for personnel and misuse of computing resources and stronger security controls on internal networks (e.g., deploying intrusion detection software to more internal networks and hosts). |
| Time per Incident | For each incident, time can be measured in several ways:   1. Total amount of labor spent working on the incident 2. Elapsed time from the beginning of the incident to incident discovery, to the initial impact assessment, and to each stage of the incident handling process (e.g., containment, recovery) 3. How long it took the incident response team to respond to the initial report of the incident 4. How long it took to report the incident to management and, if necessary, appropriate external entities (e.g., Tier-2). |
| Objective Assessment of each Incident | The response to an incident that has been resolved can be analyzed to determine how effective it was. The following are examples of performing an objective assessment of an incident:   1. Reviewing logs, forms, reports, and other incident documentation for adherence to established incident response policies and procedures 2. Identifying which precursors and indicators of the incident were recorded to determine how effectively the incident was logged and identified 3. Determining if the incident caused damage before it was detected 4. Determining if the actual cause of the incident was identified, and identifying the vector of attack, the vulnerabilities exploited, and the characteristics of the targeted or victimized systems, networks, and applications 5. Determining if the incident is a recurrence of a previous incident 6. Calculating the estimated monetary damage from the incident (e.g., information and critical business processes negatively affected by the incident) 7. Measuring the difference between the initial impact assessment and the final impact assessment 8. Identifying which measures, if any, could have prevented the incident. |
| Subjective Assessment of each Incident | Incident response team members may be asked to assess their own performance, as well as that of other team members and of the entire team. Another valuable source of input is the owner of a resource that was attacked, in order to determine if the owner thinks the incident was handled efficiently and if the outcome was satisfactory. |

Table - Metrics

# **APPENDIX H – INCIDENT RESPONSE PLAN TESTING**

**1.0 Introduction**

Although it is important to have plans in place to help an organization respond to and manage various situations involving information technology (IT), it is equally important to maintain these plans in a state of readiness. This includes having IT personnel trained to fulfill their roles and responsibilities; having plans exercised to validate their policies and procedures; and having systems tested to ensure their operability. The following types of tests will be performed on an annual basis

* Tabletop Exercise
* Functional Exercise

**2.0 Exercise Types**

**2.1 Tabletop Exercises**

Tabletop exercises are discussion-based events where personnel with roles and responsibilities in the IRP meet in a classroom setting or in breakout groups to discuss their roles during an event and their responses to a particular situation. Tabletop exercises are conducted in an informal environment, with a facilitator guiding participants through a discussion designed to meet pre-defined objectives. One or more scenarios may be discussed during a single tabletop exercise. The following methodology will be used for planning and performing IRP tabletop exercise event:



**Design**. The IRP Exercise Coordinator designs the Event. The major steps in the event design process are as follows:

1. Determine the exercise topic based on the focus of the plan being exercised
2. Determine the exercise scope based on the target audience
3. Identify the objectives of the exercise
4. Identify the individuals that should participate in the exercise and invite them to the event
5. Identify the staff for the exercise, including a facilitator and a data collector
6. Coordinate the logistics for the exercise event.

**Develop**. The IRP Exercise Coordinator creates the documentation to be used before, during, and after the exercise event. Typical documentation includes a briefing, a guide, and an after action report.

**Conduct**. In this phase, the IRP is actually exercised. Tabletop exercises are usually conducted in a classroom-type setting. The facilitator provides a briefing to the participants, then walks them through the scenario and initiates a group discussion using a question from the facilitator guide. As the discussion continues, the facilitator may inject additional questions periodically. The data collector documents issues to be included in the after action report. Immediately following the facilitated discussion, the facilitator and data collector conduct an exercise debrief, in which they ask the participants in which areas they excel, in which areas they could use additional training, and which areas of the IRP should be updated.

**Evaluate**. The comments from the debrief, along with lessons learned during the exercise, will be captured in an [after action report](#_Enclosure_1_–).

**2.2 Functional Exercises**

Functional exercises allow personnel with operational responsibilities to validate their IRP and their operational readiness for events by performing their duties in a simulated operational environment. Activities for a functional exercise are scenario-driven. Additional situations are often simulated during the course of the exercise. Functional exercises are designed to exercise specific team members, procedures, and assets involved in one or more functional aspects of the IRP. The following methodology will be used for planning and performing IRP functional exercise event:



**Design**. The IRP Exercise Coordinator designs the Event. The major steps in the event design process are as follows:

1. Determine the exercise topic based on the overarching objectives for exercising the IRP
2. Determine the exercise scope based on which portions of the IRP should be exercised
3. Identify the objectives of the exercise
4. Identify the individuals that should participate in the exercise and invite them to the event
5. Identify the staff for the exercise, including an exercise director and one or more controllers, data collectors, and simulators
6. Coordinate the logistics for the exercise event.

**Develop**. The IRP Exercise Coordinator creates the documentation to be used before, during, and after the exercise event. Typical documentation includes briefings for participants and exercise staff; a scenario; a master scenario events list (MSEL); message injects and a message inject tracking form; an after action report; and controller, data collector, and simulator books.

**Conduct**. Functional exercises are typically conducted in real or near-real time and prompt participants to carry out their roles and responsibilities as realistically as possible. A functional exercise is often initiated by a telephone call or other appropriate means, alerting selected personnel of the implementation or activation of the IRP. Participants are expected to carry out operational or decision-making activities documented in the IRP. The IRP Exercise Coordinator administers the exercise, including introducing the scenario and message injects to participants. Data collectors directly observe player actions during the exercise. Simulators assume the roles of entities that are not participating in the event, such as external organizations or private citizens. The IRP Exercise Coordinator announces the conclusion of the exercise. Immediately following the exercise play, the exercise director, controllers, and data collectors conduct an exercise debrief with the participants, requesting feedback from everyone present.

**Evaluate**. The comments from the debrief, along with lessons learned during the exercise, will be captured in an [after action report](#_Enclosure_1_–). The report should include background information about the exercise, documented observations made by the exercise staff, and recommendations for enhancing the IRP that was exercised. Outcomes of the evaluation could include updating the IRP, briefing managers on the results, and performing other actions.

# **APPENDIX I – DETAILED COMPLIANCE MATRIX**

The following table provides traceability between this document and the Assessment Procedures contained within NIST Special Publication 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations".

| Control Number | Assessment  Number | CCI  Number | Confidentiality | Integrity | Availability | Assessment Procedures | Reference |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IR-1 | IR-1 (a) | CCI-002776 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-1 | IR-1 (a) | CCI-002777 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-1 | IR-1 (a) (1) | CCI-000805 | High Moderate Low | High Moderate Low | High Moderate Low | CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meets the DoD requirements for incident response policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-1 | IR-1 (a) (1) | CCI-000806 | High Moderate Low | High Moderate Low | High Moderate Low | CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-1 | IR-1 (a) (2) | CCI-000809 | High Moderate Low | High Moderate Low | High Moderate Low | CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-1 | IR-1 (a) (2) | CCI-000810 | High Moderate Low | High Moderate Low | High Moderate Low | CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.   DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-1 | IR-1 (b) (1) | CCI-000808 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-1 | IR-1 (b) (1) | CCI-000807 | High Moderate Low | High Moderate Low | High Moderate Low | CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-1 | IR-1 (b) (2) | CCI-000812 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as reviewed annually - updated as appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-1 | IR-1 (b) (2) | CCI-000811 | High Moderate Low | High Moderate Low | High Moderate Low | CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered at the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.    DoD has defined the frequency as reviewed annually - updated as appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-10 | IR-10 | CCI-002822 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines appointments to the integrated team as well as the documented roles and responsibilities to ensure the organization being inspected/assessed establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel. | [Table 3](#Table3)  Note: Code Analysis, tool development and real-time operations are Tier-2 responsibilities and outside the scope of this Organization |
| IR-2 (1) | IR-2 (1) | CCI-000816 | High | High | High | The organization conducting the inspection/assessment obtains and examines incident response training materials and a record of training events to ensure that simulated events have been included. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IR-2 (2) | IR-2 (2) | CCI-000817 |  | High | High | The organization conducting the inspection/assessment obtains and examines the automated mechanism such as scenario-based interactive online training/CBT to verify that it provides a realistic incident response training environment. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IR-2 | IR-2 (a) | CCI-000813 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users consistent with assigned roles and responsibilities within 30 working days of assuming an incident response role or responsibility.   DoD has defined the time period as 30 working days. | [Table 3](#Table3)  [Enclosure 2](#_ENCLOSURE_2_–) |
| IR-2 | IR-2 (a) | CCI-002778 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the time period as 30 working days. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-2 | IR-2 (b) | CCI-002779 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users, other than general users, consistent with assigned roles and responsibilities when required by information system changes.   For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training. | [Table 3](#Table3)  [Enclosure 2](#_ENCLOSURE_2_–) |
| IR-2 | IR-2 (c ) | CCI-000814 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users, other than general users, consistent with assigned roles and responsibilities annually.   For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training.    DoD has defined the frequency as annually. | [Table 3](#Table3)  [Enclosure 2](#_ENCLOSURE_2_–) |
| IR-2 | IR-2 (c ) | CCI-000815 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-3 | IR-3 | CCI-001624 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines: 1. the organization's incident response plan to identify organization's testing schedule and,  2. results of previous incident response tests to ensure the organization is documenting the results IAW their incident response plan. | [Appendix G](#_APPENDIX_G_–_1)  [Appendix H](#_APPENDIX_H_–_1) |
| IR-3 | IR-3 | CCI-000818 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of test results to ensure the organization being inspected/assessed tests its incident response capability for the information system at least every six months for high availability and at least annually for low/med availability using tests and as defined in the incident response plan.   DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability.   DoD has defined the tests as tests as defined in the incident response plan. | [Appendix G](#_APPENDIX_G_–_1)  [Appendix H](#_APPENDIX_H_–_1) |
| IR-3 | IR-3 | CCI-000819 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-3 | IR-3 | CCI-000820 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the tests as tests as defined in the incident response plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-3 (1) | IR-3 (1) | CCI-000821 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the identified automated mechanisms in use to test the incident response capability for the information system. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IR-3 (2) | IR-3 (2) | CCI-002780 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the incident response testing plan to ensure the organization being inspected/assessed coordinates incident response testing with organizational elements responsible for related plans. | [Appendix H](#_APPENDIX_H_–_1) |
| IR-4 (1) | IR-4 (1) | CCI-000825 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the incident handling plan to ensure that there are procedures identified to leverage the JIMS. | [Section 3.5.1](#_3.5.1_Response_and)  [Appendix B](#Tier2Reporting)  [Table 5](#Table5)  [Table 6](#Table6)  [Table 7](#Table7)  [Table 8](#Table8) |
| IR-4 (10) | IR-4 (10) | CCI-002790 | blank | blank | blank | The organization conducting the inspection/assesment obtains and examines the documented process to ensure the organization being inspected/assessed coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IR-4 (2) | IR-4 (2) | CCI-000826 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the incident response plan and verifies it has procedures addressing dynamic reconfiguration of information system components defined in IR-4 (2), CCI 2781 as part of the incident response capability IAW CM-3. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IR-4 (2) | IR-4 (2) | CCI-002781 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components for dynamic reconfiguration as part of the incident response capability. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IR-4 (3) | IR-4 (3) | CCI-000827 | High Moderate | High Moderate | High Moderate | CJCSM 6510.01B has already identified DoD's classes of incidents.   The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the classes of incidents as classes of incidents defined in CJCSM 6510.01B Appendix A- Enclosure B.6510.01M | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-4 (3) | IR-4 (3) | CCI-000828 | High Moderate | High Moderate | High Moderate | CJCSM 6510.01B has already identified DoD's actions to take in response to classes of incidents.   The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the actions as actions defined in CJCSM 6510.01B. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-4 (4) | IR-4 (4) | CCI-000829 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines proof of the analysis (such as minutes from an incident response after action meeting or other similar activity) to ensure that incident information is being examined and correlated. | [Appendix F](#_APPENDIX_F_–) |
| IR-4 (5) | IR-4 (5) | CCI-000830 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the list of documented security violations to ensure the organization has clearly identified those violations that initiate an automated disabling or shut down of the information system.    DoD has determined the security violations are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IR-4 (5) | IR-4 (5) | CCI-000831 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure an automated mechanism is configured to disable or shutdown the information system based on the identified security violations (IR-4 (5), CCI 000830).   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 831. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IR-4 (6) | IR-4 (6) | CCI-002782 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan as well as a sampling of incident after action reports to ensure the organization being inspected/assessed implements incident handling capability for insider threats. | [G.2.0](#_G.2.0_AFTER_ACTIONS)  [Appendix F](#_APPENDIX_F_–) |
| IR-4 (7) | IR-4 (7) | CCI-002783 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed coordinates incident handling capability for insider threats across components or elements of the organization defined in IR-4 (7), CCI 2784. | [Appendix F](#_APPENDIX_F_–) |
| IR-4 (7) | IR-4 (7) | CCI-002784 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented components or elements to ensure the organization being inspected/assessed defines components or elements of the organization in which incident handling capability for insider threats will be coordinated.   DoD has determined the components or elements are not appropriate to define at the Enterprise level. | [Appendix F](#_APPENDIX_F_–) |
| IR-4 (8) | IR-4 (8) | CCI-002785 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines reports, meeting minutes, or other evidence that the organization being inspected/assessed is coordinating with external organizations defined in IR-4 (8), CCI 2786 to correlate and share incident information defined in IR-4 (8), CCI 2787 to achieve a cross-organization perspective on incident awareness and more effective incident responses. | [Appendix F](#_APPENDIX_F_–) |
| IR-4 (8) | IR-4 (8) | CCI-002786 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented external organizations to ensure the organization being inspected/assessed defines external organizations to correlate and share organization-defined incident information.  DoD has determined the external organizations are not appropriate to define at the Enterprise level. | [Appendix F](#_APPENDIX_F_–) |
| IR-4 (8) | IR-4 (8) | CCI-002787 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented incident information to ensure the organization being inspected/assessed defines what incident information will be correlated and shared with each external organization defined in IR-4 (8), CCI 2786.   DoD has determined the incident information is not appropriate to define at the Enterprise level. | [Appendix F](#_APPENDIX_F_–) |
| IR-4 (9) | IR-4 (9) | CCI-002788 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines incident response logs to ensure that they reflect the use of at a minimum, the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).   DoD has defined the dynamic response capabilities as at a minimum, the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IR-4 (9) | IR-4 (9) | CCI-002789 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the dynamic response capabilities as at a minimum, the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IR-4 | IR-4 (a) | CCI-000822 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documentation identifying the CNDSP leveraged as well as the documented procedures for incident handling to ensure that there is a certified CNDSP in use and that there are procedures implemented to handle incidents until they are transferred to the responsibility of the CNDSP. | [Section 1.2](#_1.2_Roles_and)  [Appendix B](#_APPENDIX_B_–) |
| IR-4 | IR-4 (b) | CCI-000823 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan (IR-8) and contingency plan (CP-2) to ensure they allow for an effective transfer of information system activity and maintain confidentiality and integrity of the contigency assets. | [Table 6](#Table6)  Contingency Plan (External Artifact) |
| IR-4 | IR-4 (c) | CCI-000824 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines after action reports or meeting minutes to identify actionable lessons learned to verify that lessons learned are incorporated into the plan as changes are necessary. | [Appendix G.2.0](#_G.2.0_AFTER_ACTIONS)  [Change Record](#ChangeRecord) |
| IR-4 | IR-4 (c) | CCI-001625 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines  recent changes to the incident response plan (based on IR-4, CCI 000824) to verify that they have been disseminated and reviews the most recent after action report to ensure that changes have been followed. | [Appendix G.2.0](#_G.2.0_AFTER_ACTIONS)  [Change Record](#ChangeRecord) |
| IR-5 | IR-5 | CCI-000832 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident handling plan to ensure that there are procedures identified to leverage the JIMS. | [Section 3.5.1](#_3.5.1_Response_and)  [Appendix B](#Tier2Reporting)  [Table 5](#Table5)  [Table 6](#Table6)  [Table 7](#Table7)  [Table 8](#Table8) |
| IR-5 (1) | IR-5 (1) | CCI-000833 | High | High | High | The organization conducting the inspection/assessment obtains and examines the incident handling plan to ensure that there are procedures identified to leverage the JIMS. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IR-5 (1) | IR-5 (1) | CCI-001626 | High | High | High | The organization conducting the inspection/assessment obtains and examines the incident handling plan to ensure that there are procedures identified to leverage the JIMS. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IR-5 (1) | IR-5 (1) | CCI-001627 | High | High | High | The organization conducting the inspection/assessment obtains and examines the incident handling plan to ensure that there are procedures identified to leverage the JIMS. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IR-6 (1) | IR-6 (1) | CCI-000837 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the incident handling plan to ensure that there are procedures identified to leverage the JIMS. | [Section 3.5.1](#_3.5.1_Response_and)  [Appendix B](#Tier2Reporting)  [Table 5](#Table5)  [Table 6](#Table6)  [Table 7](#Table7)  [Table 8](#Table8) |
| IR-6 (2) | IR-6 (2) | CCI-000838 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines a sample of previous security incidents to ensure the associated vulnerabilities were reported to personnel defined in IR-6 (2), CCI 2792 IAW the incident response plan (IR-8). Reporting shall be conducted IAW CJCSM 6510.01B. | [Appendix G.2.0](#_G.2.0_AFTER_ACTIONS)  [Appendix A](#_APPENDIX_A_–)  [Appendix B](#_APPENDIX_B_–)  [Appendix C](#_APPENDIX_C_–) |
| IR-6 (2) | IR-6 (2) | CCI-002792 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented personnel to ensure the organization being inspected/assessed defines personnel or roles to whom information system vulnerabilities associated with reported security incident information are reported IAW CJCSM 6510.01B. | [Table 3](#Table3)  [Appendix A](#_APPENDIX_A_–)  [Appendix B](#_APPENDIX_B_–)  [Appendix C](#_APPENDIX_C_–) |
| IR-6 (3) | IR-6 (3) | CCI-002793 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IR-6 | IR-6 (a) | CCI-000834 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.    DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance.   The organization conducting the inspection/assessment obtains and examines the incident response plan to determine if more stringent response time requirements have been identified. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-6 | IR-6 (a) | CCI-000835 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the user agreement to ensure users are required to report suspected security incidents to the organizational incident response capability within the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance.   DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. | SAAR (external artifact)  [Appendix B](#_APPENDIX_B_–)  [Table 7](#Table7) |
| IR-6 | IR-6 (b) | CCI-000836 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines a sample of previous security incidents to ensure the incidents were reported to the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT) any security incidents IAW the incident response plan (IR-8). Reporting shall be conducted IAW CJCSM 6510.01B.    DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT). | [Appendix G.2.0](#_G.2.0_AFTER_ACTIONS)  [Appendix A](#_APPENDIX_A_–)  [Appendix B](#_APPENDIX_B_–)  [Appendix C](#_APPENDIX_C_–) |
| IR-6 | IR-6 (b) | CCI-002791 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT). | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-7 | IR-7 | CCI-000839 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment will interview organizational users to determine awareness of incident response support services and quality of assistance of those services when used. If interviewing organizational users is not feasible, then review users manuals/documentation to ensures it identifies an incident response support service to contact. | [Table 3](#Table3) |
| IR-7 (1) | IR-7 (1) | CCI-000840 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the incident response information sharing capability to validate the information sharing capability is available to organizational users. | Internal Web Portal (external link) |
| IR-7 (2) | IR-7 (2) (a) | CCI-000841 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the formal agreement document between the organization and CNDSP to validate it is current and valid. | [Table 3](#Table3) |
| IR-7 (2) | IR-7 (2) (b) | CCI-000842 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the list of internal incident response team members to validate it is accurate and current. Interviews with CNDSP personnel and organizational incident response team members may also be conducted. | [Section 1.2](#_1.2_Roles_and) |
| IR-8 | IR-8 (a) | CCI-002794 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented incident response plan to ensure the organization being inspected/assessed develops an incident response plan. | This document |
| IR-8 | IR-8 (a) (1) | CCI-002795 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed provides within their plan, a roadmap for implementing its incident response capability. | [Section 1.1](#_1.1_Applicability) |
| IR-8 | IR-8 (a) (2) | CCI-002796 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed describes within their plan, the structure and organization of the incident response capability. | [Section 1.2](#_1.2_Roles_and) |
| IR-8 | IR-8 (a) (3) | CCI-002797 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed provides within their plan, a high-level approach for how the incident response capability fits into the overall organization. | [Section 1.1](#_1.1_Applicability) |
| IR-8 | IR-8 (a) (4) | CCI-002798 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure it meets the unique requirements of the organization being inspected/assessed, which relate to mission, size, structure, and functions. | [Section 1.1](#_1.1_Applicability) |
| IR-8 | IR-8 (a) (5) | CCI-002799 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines reportable incidents IAW CJCSM 6510.01B Table B-A-2. | [Appendix A](#_APPENDIX_A_–)  [Appendix B](#_APPENDIX_B_–) |
| IR-8 | IR-8 (a) (6) | CCI-002800 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines metrics for measuring the incident response capability within the organization IAW CJCSM 6510.01B, Enclosure A. | [Appendix G.3.0](#_G.3.0_METRICS) |
| IR-8 | IR-8 (a) (7) | CCI-002801 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines within their plan, the resources and management support needed to effectively maintain and mature an incident response capability. | [Section 1.1](#_1.1_Applicability)  [Section 1.2](#_1.2_Roles_and) |
| IR-8 | IR-8 (a) (8) | CCI-000844 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan to validate it has been properly signed by at a minimum, the ISSM and ISSO.   DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO. | [Signatures](#Signatures) |
| IR-8 | IR-8 (a) (8) | CCI-002802 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-8 | IR-8 (b) | CCI-000846 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines organizationally approved information sharing mechanism to validate all stakeholders identified in the incident response plan have adequate access to the incident response plan.   DoD has defined the list as all stakeholders identified in the incident response plan. | Internal Web Portal (external link) |
| IR-8 | IR-8 (b) | CCI-000845 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the list as all stakeholders identified in the incident response plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-8 | IR-8 (c) | CCI-000848 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the incident response plan to validate it is current and has been reviewed within the last year.   DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents). | [Change Record](#ChangeRecord) |
| IR-8 | IR-8 (c) | CCI-000847 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents). | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-8 | IR-8 (d) | CCI-000849 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines documentation of the update actions for the incident response plan to ensure the organization is updating the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing and incorporating lessons learned from past incidents (IR-4a). | [Change Record](#ChangeRecord)  [Appendix G](#_APPENDIX_G_–_1)  [Appendix H](#_APPENDIX_H_–_1) |
| IR-8 | IR-8 (e ) | CCI-002803 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-8 | IR-8 (e) | CCI-000850 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment examines the incident response plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been communicated to all stakeholders identified in the incident response plan, not later than 30 days after the change is made.   DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made. | [Change Record](#ChangeRecord)  Internal Web Portal (external link) |
| IR-8 | IR-8 (f) | CCI-002804 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines artifacts which identify how the incident response plan is protected to ensure the organization being inspected/assessed protects the incident response plan from unauthorized disclosure and modification. | Internal Web Portal (external link) |
| IR-9 (1) | IR-9 (1) | CCI-002813 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines appointment letters to ensure the organization being inspected/assessed appoints personnel or roles defined in IR-9 (1), CCI 2815 as having the responsibility for responding to information spills. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 (1) | IR-9 (1) | CCI-002815 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines personnel or roles to whom responsibility for responding to information spills will be assigned, which must include the ISSO and ISSM.    DoD has determined the personnel or roles are not appropriate to define at the Enterprise level. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 (2) | IR-9 (2) | CCI-002816 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the training records for a sampling of incident response personnel to ensure the organization being inspected/assessed provides information spillage response training annually.   DoD has defined the frequency as annually. | [Enclosure 2](#_ENCLOSURE_2_–) |
| IR-9 (2) | IR-9 (2) | CCI-002817 | High Moderate Low |  |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-9 (3) | IR-9 (3) | CCI-002818 |  |  | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented procedures defined in IR-9 (3), CCI 2819 as well as after action reports of incidents to ensure the organization being inspected/assessed implements procedures defined in IR-9 (3), CCI 2819 to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 (3) | IR-9 (3) | CCI-002819 |  |  | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented procedures to ensure the organization being inspected/assessed defines procedures to implement to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.   DoD has determined the procedures are not appropriate to define at the Enterprise level. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 (4) | IR-9 (4) | CCI-002820 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs security safeguards defined in IR-9 (4), CCI 2821 for personnel exposed to information not within assigned access authorizations. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 (4) | IR-9 (4) | CCI-002821 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines security safeguards to employ for personnel exposed to information not within assigned access authorizations.   DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 | IR-9 (a) | CCI-002805 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that specific information involved in the information system contamination is identified. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 | IR-9 (b) | CCI-002806 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that at a minimum, the OCA, the information owner/originator, the ISSM, the activity security manager, and the responsible computer incident response center were alerted of the information spill using a method of communication not associated with the spill.   DoD has defined the personnel or roles as at a minimum, the OCA, the information owner/originator, the ISSM, the activity security manager, and the responsible computer incident response center. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 | IR-9 (b) | CCI-002807 | High Moderate Low |  |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the OCA, the information owner/originator, the ISSM, the activity security manager, and the responsible computer incident response center. | Automatically compliant with this CCI because they are covered at the DoD level |
| IR-9 | IR-9 (c ) | CCI-002808 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that the organization being inspected/assessed isolates contaminated information system or system component. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 | IR-9 (d) | CCI-002809 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that the organization being inspected/assessed eradicates the information from the contaminated information system or component. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 | IR-9 (e ) | CCI-002810 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that the organization being inspected/assessed identifies other information systems or system components that may have been subsequently contaminated. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 | IR-9 (f) | CCI-002811 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to ensure that the organization being inspected/assessed performs actions defined in IR-9, CCI 2812. | [Section 4](#_4.0_INFORMATION_SPILLS) |
| IR-9 | IR-9 (f) | CCI-002812 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented additional actions to ensure the organization being inspected/assessed defines other actions required to respond to information spills.   DoD has determined the actions are not appropriate to define at the Enterprise level | [Section 4](#_4.0_INFORMATION_SPILLS) |

# **ENCLOSURE 1 – AFTER ACTIONS REPORT TEMPLATE**

**After Actions Report**

**1.0 Introduction**

On {DATE}, {ACRONYM} participated in a tabletop exercise designed to validate their understanding of the {ACRONYM} Incident Response Plan.

**2.0 Objectives**

The exercise objectives are as follows:

* Validate the team’s ability to respond to security incidents
* Validate the accuracy of procedures documented in the {ACRONYM} Incident Response Plan
* Identify areas of the {ACRONYM} Incident Response Plan that need to be revised.

**3.0 Agenda**

|  |  |
| --- | --- |
| Date | {DATE} |
| Location | {LOCATION} |
| Exercise Name | {EXERCISE NAME} |
| {TIME} | Welcoming Remarks and Introductions |
| {TIME} | Exercise Briefing (Objectives, Rules of Engagement, etc.) |
| {TIME} | Scenario Discussion |
| {TIME} | Debrief/Hotwash |

**4.0 Discussion of Findings**

The {EXERCISE NAME} provided information on the {ACRONYM} Incident Response Plan. An important benefit of the exercise was the opportunity for participants to raise important questions, concerns, and issues. The discussion findings from the exercise along with any necessary recommended actions are as follows:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Subject | Observation | Recommendations |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |

# **ENCLOSURE 2 – TRAINING RESOURCES**

Incident response training to information system users, other than general users, consistent with assigned roles and responsibilities is a key principle to ensure a successful IRP implementation.

For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training.

The below resources have been compiled to assist with IRP training requirements. Additional, commercial-based training, may be used to supplement in-house DoD provided training.

**Incident Response**

* eLearning: [Introduction to DoD IDS Analysis](http://www.cdse.edu/catalog/elearning/DS-IA105.html) DS-IA105.06
* eLearning: [DoD Intrusion Detection System (IDS) Analysis Part II](http://www.cdse.edu/catalog/elearning/DS-IA107.html) DS-IA107.06
* [ODAA Process Manual: Incident Response (Section 4.5)](http://www.dss.mil/documents/odaa/ODAA%20Process%20Manual%20Version%203.2.pdf#page=44) PDF icon
* Webinar: [Reportable Unclassified Cyber Events](http://www.cdse.edu/catalog/webinars/counterintelligence/reportable-events.html)
* eLearning: [Windows Server 2003 Incident Preparation & Response (IP&R)](http://www.cdse.edu/catalog/elearning/DS-IA300.html) DS-IA300.06

**Data Spills**

* [ODAA Process Manual: C&A Process, Operational Controls (Section 4.0)](http://www.dss.mil/documents/odaa/ODAA%20Process%20Manual%20Version%203.2.pdf#page=40) PDF icon
* [ODAA Process Manual: Contamination Cleanup Procedures (Section 4.5.6)](http://www.dss.mil/documents/odaa/ODAA%20Process%20Manual%20Version%203.2.pdf#page=48) PDF icon
* [CNSSI 1001 National Instruction on Classified Information Spillage](http://www.cdse.edu/documents/toolkits-cybersecurity/cnssi1001-classified-info-spillage.pdf) PDF icon
* [DoDM 5200.01, Vol 3, DoD Information Security Program: Protection of Classified Information, February 24, 2012](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf) PDF icon
* Short: [Data Spills](http://www.cdse.edu/toolkits/cybersecurity/incident.html)

**Administrative Inquiry**

* [Administrative Inquiry (AI) Guidelines for Information Systems (IS)](http://www.dss.mil/documents/odaa/administrative_inquiry.pdf) PDF icon
* [Administrative Inquiry (AI) Job Aid for Industry](http://www.cdse.edu/documents/cdse/ai-job-aid-for-industry.pdf) PDF icon

**Insider Threat Training**

* eLearning: [Insider Threat Awareness](http://www.cdse.edu/catalog/elearning/CI121.html) CI121.16
* eLearning: [Establishing an Insider Threat Awareness Program for your Organization](http://www.cdse.edu/catalog/elearning/CI122.html) CI122.06
* eLearning: [Counterintelligence Awareness & Reporting Course for DoD Employees](http://www.cdse.edu/catalog/elearning/CI116.html) CI116.06
* eLearning: [Integrating CI and Threat Awareness into Your Security Program](http://www.cdse.edu/catalog/elearning/CI010.html) CI010.16
* eLearning: [NISP Reporting Requirements](http://www.cdse.edu/catalog/elearning/IS150.html) IS150.16
* eLearning: [Defense Cyber Investigation Training Academy - Cyber Insider Threat Analysis Course](https://www.dcita.edu/courses.html)
* Webinar: [Insider Threat](http://www.cdse.edu/catalog/webinars/counterintelligence/insider-threat.html)
* Webinar: [Potential Espionage Indicators (PEI): Detecting Actions Outside the Norm](http://www.cdse.edu/catalog/webinars/counterintelligence/potential-espionage-indicators.html)
* Webinar: [Cyber Insider Threat](http://www.cdse.edu/catalog/webinars/cyber-security/cyber-insider-threat.html)
* Short: [CI Concerns for Adjudicators Short](http://www.cdse.edu/shorts/counterintelligence.html)
* [DNI/NCIX Instructor led: Establishing and Operating an Insider Threat Detection Program](http://www.ncix.gov/training/courses.php)
* [DNI/NCSC Video Series: Terminal Risk](http://www.ncix.gov/index.php)

**Insider Threat Job Aids**

* [DSS Insider Threat Brochure](http://www.dss.mil/documents/ci/Insider-Threats.pdf) PDF icon
* [DSS Elicitation and Recruitment Brochure](http://www.dss.mil/documents/ci/Elicitation.pdf) PDF icon
* [DoD Hotline Posters](http://www.dodig.mil/hotline/posters.cfm)
* [DHS - NIAC - National Infrastructure Advisory Council Final Report & Recommendations on The Insider Threat to Critical Infrastructures (NIAC, Apr 8, 2008)](http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf) PDF icon
* [Espionage and Other Compromises of National Security 1975-2008 PERSEREC Case Studies](http://www.dhra.mil/perserec/espionagecases/index.html)
* [FBI Brochure - The Insider Threat: A guide to detecting and deterring an insider spy](http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure) PDF icon
* [FBI - Insider Threat Page](http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat)
* [Insider Threat Case Study - Yuan Li](http://www.cdse.edu/documents/cdse/CDSE-Insider-Threat-Case-Study-Yuan-Li.pdf)
* [Insider Threat Case Study - Bryan Underwood](http://www.cdse.edu/documents/cdse/CDSE-Insider-Threat-Case-Study-Bryan-Underwood.pdf)
* [Security Posters](http://www.cdse.edu/resources/posters.html)
* [Secret Service - National Threat Assessment Center - Insider Threat Study](http://www.secretservice.gov/ntac_its.shtml)
* [PERSEREC Insider Risk Evaluation & Audit Tool](http://www.dhra.mil/perserec/products.html)
* [PERSEREC Adjudicative Desk Reference](http://www.dhra.mil/perserec/adr/ADR_Version_4.pdf) PDF icon

**Insider Threat Best Practices**

* [National Insider Threat Task Force](http://www.ncix.gov/nittf/index.php)
* [Insider Threat Best Practices - The CERT Insider Threat Center](http://www.cert.org/insider-threat/best-practices/index.cfm)
* [GAO Report: Insider Threats - June 2015](http://www.cdse.edu/documents/toolkits-insider/insider-threat-gao-jun-2015.pdf)
* [The CERT Top Ten List for Winning the Battle Against Insider Threats](http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=52423)