CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

Directive Current as of 18 December 2014

J-6
DISTRIBUTION: A, B, C, JEL, S

CJCSM 6510.01B
10 July 2012

CYBER INCIDENT HANDLING PROGRAM

References: See Enclosure H.

1. Purpose. This manual describes the Department of Defense (DoD) Cyber Incident Handling Program and specifies its major processes, implementation requirements, and related U.S. government interactions.

2. Cancellation. CJCSM 6510.01A, 24 June 2009, "Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program)," is canceled.

3. Applicability. This manual applies to the Joint Staff and to Combatant Commands, Services, Defense agencies, DoD field activities, and joint and combatant activities (hereafter referred to as CC/S/A/FAs).

4. Procedures. See Enclosures A through G.

5. Summary of Changes

a. Updates manual to include the new mission, processes, and procedures of U.S. Cyber Command (USCYBERCOM), the subunified command of U.S. Strategic Command (USSTRATCOM).

b. Updates manual based on Unified Command Plan (UCP) Change 1, 12 September 2011.

6. Releasability. This manual is approved for public release; distribution is unlimited. DoD components (to include the Combatant Commands), other federal agencies, and the public may obtain copies of this manual through the Internet from the CJCS Directives Home Page--
http://www.dtic.mil/cjcs_directives.

7. Effective Date. This manual is effective immediately.

WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

Enclosures:
A—Cyber Incident Handling Program
B—Cyber Incident Handling Methodology
C—Cyber Incident Reporting
D—Cyber Incident Analysis
E—Cyber Incident Response
F—Collaboration with Other Strategic Communities
G—Computer Network Defense Incident Handling Tools
H—References
GL—Glossary

DISTRIBUTION

Distribution A, B, C, and JEL plus the following:

	Copies
Director, NSA/CSS Threat Operations Center	1
Director of Current Operations, Army Cyber Command	1
Director of Current Operations, Tenth Fleet	1
Director of Current Operations, Marine Forces Cyber Command	1
Director of Current Operations, 24th Air Force	1
Director of Current Operations, Coast Guard Cyber Command	1
Director, Army Research Laboratory	1
Director, High Powered Computing Center Management Office	1
Director, U.S. Strategic Command J6	1

The office of primary responsibility for the subject directive has chosen electronic distribution to the above organizations via e-mail. The Joint Staff Information Management Division has responsibility for publishing the subject directive to the SIPRNET and NIPRNET Joint Electronic Library (JEL) Web sites.

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

Page

ENCLOSURE A CYBER INCIDENT HANDLING PROGRAM

ENCLOSURE B CYBER INCIDENT HANDLING METHODOLOGY

APPENDIX A TO ENCLOSURE B CYBER INCIDENT AND REPORTABLE CYBER EVENT CATEGORIZATION

ENCLOSURE C CYBER INCIDENT REPORTING

APPENDIX A TO ENCLOSURE C REPORTING TIMELINES

APPENDIX B TO ENCLOSURE C GENERAL CYBER INCIDENT REPORT FORMAT

Page

APPENDIX C TO ENCLOSURE C CYBER INCIDENT REPORTING DIAGRAMS

ENCLOSURE D CYBER INCIDENT ANALYSIS

APPENDIX A TO ENCLOSURE D DELIVERY VECTORS

APPENDIX B TO ENCLOSURE D SYSTEM WEAKNESSES

APPENDIX C TO ENCLOSURE D IMPACT ASSESSMENT MATRIX

ENCLOSURE E CYBER INCIDENT RESPONSE

Page

TABLES

ENCLOSURE A

CYBER INCIDENT HANDLING PROGRAM

1. Introduction

a. Purpose

(1) The Department of Defense maintains a comprehensive cyber incident handling program.

(2) This program ensures an integrated capability to continually improve the Department of Defense's ability to rapidly identify and respond to cyber incidents that adversely affect DoD information networks and information systems (ISs). It does so in a way that is consistent, repeatable, quality driven, measurable, and understood across DoD organizations.

(3) This enclosure provides requirements and methodology for establishing, operating, and maintaining a robust DoD cyber incident handling capability for routine response to events and incidents within the Department of Defense. Additional guidance for cyber incident handling for a crisis or in case of active hostilities will be issued by USCYBERCOM as required.

b. Background

(1) DoD information networks, including Defense Industrial Base (DIB) networks, face a full range of Internet threats, including advanced and persistent threats that can evade commercially available security tools and defeat generic security best practices.

(2) In this dynamic environment, it is critical that those responsible for building, operating, defending, maintaining, and ensuring the continuity of these information networks maintain a unified and resilient capability to minimize the impact of these threats on mission operations. This capability must be able to adapt over time to changes in the threat environment.

(3) The threat from adversaries to DoD information degrades the Department of Defense's ability to maintain current and future warfighting capabilities.

(4) This threat also severely hinders the ability to maintain a high level of confidence in net-centric operations relied upon by all levels of personnel, from generals to Soldiers on the ground.

(5) While this threat cannot be completely eliminated and will likely evolve over time, it is crucial to maintain a proactive, progressive, and coordinated approach to detecting and responding to cyber events and incidents that can adversely affect DoD information networks and ISs.

(6) Federal agencies are required to have in place cyber incident handling mechanisms in accordance with (IAW) the Federal Information Security Management Act (FISMA) (reference a) and Appendix III, Office of Management and Budget (OMB) Circular No. A-130, "Management of Federal Information Resources" (reference b).

(7) Computer Network Defense Service Providers (CNDSPs)

(a) The Department of Defense requires Tier II CNDSPs to provide three services: (1) protect; (2) monitor, analyze, and detect; and (3) respond IAW DoD Instruction (DoDI) O-8530.2, "Support to Computer Network Defense (CND)" (reference c).

(b) These services must be certified, accredited, and sustained at an acceptable level of quality for their subscribers.

(8) The Department of Defense developed the Cyber Incident Handling Program to provide specific guidance for CC/S/A/FAs regarding the requirements for cyber incident handling and reporting.

c. Scope

(1) The Department of Defense is a global presence composed of multiple military commands, agencies, organizations, and functions that must coordinate, manage, and respond to technology threats, attacks, and incidents—any of which could, without proper controls to protect, detect, and manage their effects, adversely affect DoD information networks and ISs. It is therefore critical that appropriate guidance be developed and disseminated to CC/S/A/FAs responsible for effectively and efficiently managing these information networks, ISs, and the DIB.

(2) It is the responsibility of the network defenders and users to ensure the security of computing and communication systems for executing successful military operations and maintaining the integrity of information within the cyber domain and throughout the Department of Defense.

(3) This enclosure provides overarching guidance that fosters a shared and thorough understanding of how the Department of Defense's global, regional, and local organizations coordinate efforts to positively affect response actions.

(4) Effective response requires consistent and complete end-to-end reporting using a framework that enables tactical and strategic analytical functions. These functions help to characterize the threat environment and support development and implementation of effective countermeasures to protect and defend DoD information networks and information. Maintaining the availability, confidentiality, and integrity of DoD information networks and information to support DoD operations is critical for national security.

(5) 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 (reference ff). This document is a framework that will be used by DoD entities 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 Department of Defense's ability to protect and defend DoD information networks and information.

2. Roles and Responsibilities

a. Joint Staff and CC/S/A/FAs will:

(1) Comply with DoD Cyber Incident Handling Program responsibilities IAW reference d, CJCSI 6510.01, "Information Assurance (IA) and Support to Computer Network Defense (CND)," and DoDI O-8530.2 (reference c).

(2) Document and report events and incidents IAW this manual.

(3) Ensure Tier II CNDSPs are established or appointed and registered with DISA to provide CND services for CC/S/A/FA information networks and ISs.

(4) Coordinate horizontally and vertically with appropriate organizations (e.g., Tiers I, II, and III; law enforcement/counterintelligence (LE/CI); and the Intelligence Community (IC)) for cyber incidents.

(5) Comply with orders and directives (including, but not limited to, OPORDS, WARNORDs, FRAGOs, TASKORDs, and other approved order formats).

(6) Include requirements to comply with all portions of this program and stipulate its enforcement within DoD information technology (IT)/service contracts. CC/S/A/FAs, vendors, contractors, and suppliers must comply with the procedures contained in this manual.

(7) Coordinate with USCYBERCOM, through its Tier II CNDSP, on cyber incidents prior to taking action outside the Department of Defense, consistent with National Security Presidential Directive 38 and the Trilateral Memorandum of Agreement.

(8) Coordinate with the Defense Intelligence Agency (DIA), National Security Agency/Central Security Service Threat Operations Center (NTOC), and appropriate DoD agency centers on cyber incidents involving intelligence systems prior to coordinating or taking actions outside the Department of Defense consistent with Enclosure F.

b. USSTRATCOM will:

(1) Direct operation and defense of DoD information networks IAW the UCP (reference e).

(2) Execute cyberspace operations as directed.

(3) Delineate USCYBERCOM responsibilities to:

(a) Issue cyber incident or reportable event response orders and alerts through USCYBERCOM to the CC/S/A/FAs.

(b) Coordinate with the IC Incident Response Center (IC-IRC), which operates under the authority of the IC Chief Information Officer (CIO), on matters relating to the governance, secure operations, and defense of the IC networks.

(c) Coordinate with the Department of Homeland Security (DHS) and other federal agencies for incidents related to cyberspace involving the Department of Defense. As appropriate, notify and/or coordinate with the United States Computer Emergency Readiness Team (US-CERT) on cyberspace incidents.

(d) Coordinate with USNORTHCOM, National Guard Bureau, and USPACOM for cyber incidents that involve the DHS and other federal agencies where Defense Support of Civil Authorities is involved.

(e) Maintain and disseminate DoD intrusion detection system (IDS) signature sets for DoD level sensors (Tier I) and provide necessary threat information to assist Tier II and Tier III CNDSP organizations developing IDS signature sets for their sensors.

(f) Provide reports (summaries, significant cyber incidents, trends, enterprise-wide issues) to the Office of the Secretary of Defense (OSD) and Joint Staff through USSTRATCOM and to CC/S/A/FAs as necessary.

3. Computer Network Defense Overview

a. Cyber Incident Handling Program. The DoD Cyber Incident Handling Program is a component of the overall Computer Network Defense (CND) strategy for the Department of Defense. The Cyber Incident Handling Program aligns with the three services of CND IAW DoDI O-8530.2 (reference c):

(1) Protect.

(2) Monitor, analyze, and detect.

(3) Respond.

b. Cyber Incident Handling. To protect the interests of national security, cyber incidents must be coordinated among and across DoD organizations and sources outside the Department of Defense, such as LE/CI, IC, DIB partners, and critical infrastructure and critical infrastructure sector Information Sharing and Analysis Centers (ISACs). Where applicable, this document attempts to draw relationships among these services to foster a common understanding of the process by everyone responsible for directing and coordinating cyber incident response efforts.

c. CND Framework

(1) CND directs the actions taken, within the Department of Defense, to protect, monitor, analyze, detect, and respond to unauthorized activity within

DoD information networks and ISs. CND protection activity employs IA principles and security controls, and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information.

(2) The Department of Defense is organized into three tiers to conduct CND.

(a) Tier I (Global). This tier provides DoD-wide CND operational direction or support to CC/S/A/FAs. Tier I entities include USCYBERCOM as a USSTRATCOM subunified command including supporting entities such as the Defense Criminal Investigative Organization, NTOC, and appropriate DoD LE/CI organizations.

(b) Tier II (Regional/Theater). Tier II provides DoD component-wide operational direction or support and responds to direction from Tier I. Tier II includes CC/S/A/FA CNDSPs designated by heads of components to coordinate component-wide CND.

(c) Tier III (Local). Tier III provides local operational direction or support and responds to direction from a designated Tier II entity. Tier III includes bases, posts, camps, stations, and all entities responding to direction from a CC/S/A/FA Tier II CNDSP (e.g., manage and control information networks, ISs, and services, either deployed or fixed at DoD installations).

4. CND Services. As defined in DoDI O-8530.2 (reference c), there are three primary CND services: (1) protect; (2) monitor, analyze, and detect; and (3) respond.

a. These services define actions employed to prevent or lessen cyber attacks that may disrupt, deny, degrade, destroy, exploit, allow unauthorized access to, or facilitate information theft from DoD information networks, ISs, or their contents. A fourth area, capability sustainment, reflects actions that the CC/S/A/FA or its designated CNDSP must perform to ensure services are provided. CC/S/A/FAs must acquire these CND services through service relationships with CNDSPs. The CND services are enumerated and illustrated in Table A-1 (Computer Network Defense (CND) Framework).

b. CND Protection Services

(1) CND protection services include managing DoD's Cyber Condition (CYBERCON) system and creating or enhancing an information network or IS's configuration or assurance posture in response to a CND alert or threat.

(2) Protection services are often proactive (e.g., red teaming, subscriber protection, and training) and may or may not result from a cyber incident.

COMPUTER NETWORK DEFENSE FRAMEWORK			
PROTECT	**MONITOR, ANALYZE, AND DETECT**	**RESPOND**	**CAPABILITY SUSTAINMENT**
Vulnerability Scanning Support CND External Assessments Malware Protection Support Subscriber Protection Support and Training CYBERCON Implementation Information Assurance Vulnerability Management (IAVM)	Network Security Monitoring/Intrusion Detection Attack Sensing and Warning (AS&W) Indications and Warnings (I&W)/Situational Awareness	Incident Reporting Incident Response Incident Analysis	MOUs and Contracts CND Policies/Procedures CND Technology Development, Evaluation and Implementation Personnel Levels and Training/Certification Security Administration CNDSP Information Systems

Table A-1. Computer Network Defense Framework

c. CND Monitor, Analyze, and Detect Services

(1) CND monitor, analyze, and detect services provide CND situational awareness, attack sensing and warning (AS&W), and indications and warning (I&W).

(2) Multiple communities within the Department of Defense (e.g., network operations, CND services, intelligence, CI, and LE) contribute to situational awareness.

(3) AS&W data gives the Department of Defense the ability to sense changes in DoD information networks. AS&W includes the detection, correlation, identification, and characterization of a large spectrum of intentional unauthorized activity, including an intrusion or attack. It couples

these activities with notification to command and decision-makers so they can develop an appropriate response. AS&W is enabled through a managed network of intrusion, misuse, and anomaly detection systems, supporting data fusion and analysis, diagnostics, long-term trend and pattern analysis, and warning communications channels and procedures.

(4) I&W data gives the Department of Defense the ability to sense changes in adversary activities. I&W includes those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to U.S. citizens abroad. The IC provides I&W for foreign threats from nation states and transnational groups.

(5) The LE community investigates criminal activity and disseminates threat data that may pertain to domestic or foreign individuals and groups who constitute threats to the Department of Defense. The CI community conducts investigations, collections, operations, functional services, and analysis that may result in the dissemination of threat data relative to information gathered and cyber activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations by or on the behalf of foreign governments or elements thereof, foreign intelligence and security services, foreign organizations, foreign persons, or international terrorist activities.

d. CND Response Services

(1) CND response services include the actions taken to report, analyze, coordinate, and respond to any event or cyber incident for the purpose of mitigating any adverse operational or technical impact.

(2) Cyber incident reporting includes a well-defined framework for the timely reporting of any cyber event or incident. The report provides an accurate, meaningful, and complete understanding of the cyber incident from initial detection to analysis and remediation. This information feeds into the User-Defined Operational Picture, which provides local, intermediate, and DoD-wide situational awareness of CND actions and their impact.

(3) Cyber incident analysis identifies several critical elements of an incident to determine and characterize its possible effects on DoD information networks, operational missions, and other defense programs. This activity relies on effective acquisition, preservation, and timely reporting of cyber incident data.

(4) Cyber incident response includes the coordinated development and implementation of courses of action (COAs) that focus on containment, eradication, and recovery. At the same time, it ensures the acquisition and

preservation of data required for tactical analysis, strategic analysis, and/or LE investigations.

5. CND Sustainment Functions. CND sustainment functions are designed to ensure the provider continues to provide CND services to all subscribers at an acceptable level of quality and are a component of the overall DoD CND strategy. They are also an integral part of the CNDSP certification and accreditation process per the CNDSP Evaluator Scoring Metrics (v8.0) (reference oo), which include:

a. Eighteen Priority I metrics.

b. Fourteen Priority II metrics.

c. Twelve Priority III metrics.

d. Seven Priority IV metrics.

(INTENTIONALLY BLANK)

ENCLOSURE B

CYBER INCIDENT HANDLING METHODOLOGY

1. Introduction

a. 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.

b. 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.

c. Given the diverse, highly distributed, and complex environment in which the Department of Defense operates, the means by which CC/S/A/FAs implement this methodology may vary depending on the resources, technical capabilities, and local policies/procedures provided by the command authority.

d. It is expected that CC/S/A/FAs will implement and institutionalize the guidance, procedures, and policies described in this methodology in a way that yields the intended results (as described throughout) and sustains the global, regional, and local capabilities necessary to maintain and operate a robust and effective cyber incident handling program.

e. The primary objectives of the cyber incident handling process are 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.

f. All tiers must cooperate with each other (and other organizations when appropriate). This cooperation is critical to sustaining a robust cyber incident handling capability.

(1) The quality, timeliness, and consistency of reporting across all the tiers do much to determine the overall effectiveness of DoD incident handling.

(2) Effective reporting practices ensure the availability of valuable data to help military decision making and shape tactical and strategic response actions.

(3) Incident response requires coordination across various CC/S/A/FAs and is similar to coordination for other military operations.

(4) Sometimes intelligence and technical information may come from sources unique to the CND environment, including sources outside the Department of Defense. Consequently, extensive coordination can be required with the US-CERT, LE/CI organizations, the IC, industry partners, and critical infrastructure such as electric power supply system providers,

telecommunications backbone providers, transportation management systems providers, etc.

(5) Critical Infrastructure. DoD operations depend on the availability and robustness of numerous critical infrastructure elements. The first manifestation of interference with DoD operations might appear in such systems. As a result, DoD installations and organizations should maintain awareness of the status of the critical infrastructure components upon which they depend. In addition, cyber incidents that impact critical infrastructure components upon which the DoD depends should be entered into an appropriate reporting channel (US-CERT, local LE, etc.) in a timely manner to allow all parties to maintain situational awareness of the nation's cyber posture.

(6) It is imperative that information related to incidents be protected to prevent adversaries from determining impact or lack thereof. CC/S/A/FAs shall coordinate with their operations security (OPSEC) personnel to ensure appropriate OPSEC countermeasures are in place.

2. Cyber Incident Handling Process and Life Cycle

a. 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.

b. Figure B-1 illustrates the relationship of each phase to other life cycle phases. The life cycle is circular. What is learned throughout the process can be leveraged to improve the state of the practice in defending against future attacks. However, many of these activities can happen in parallel or sequentially. Figure B-2 illustrates how these activities overlap with each other.

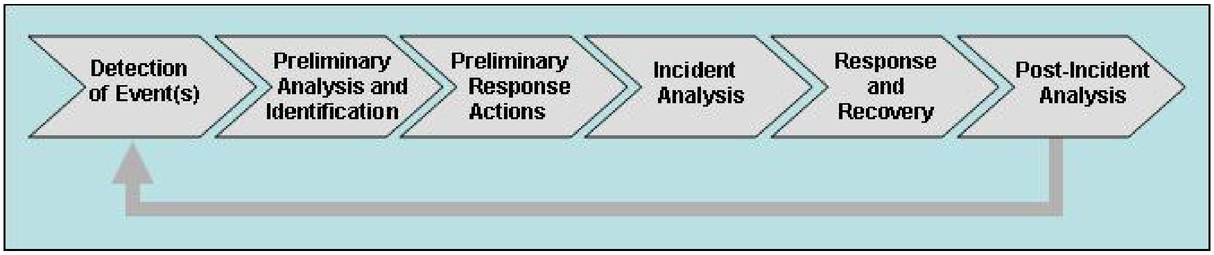


Figure B-1. Cyber Incident Life Cycle

c. Several supporting activities cross any one stage in the life cycle.

(1) Reporting and Notification

(a) Those responsible for incident handling activities must constantly refine their ability to assess an incident as it unfolds, handle the information appropriately (e.g., within security, legal, and investigative contexts), and rapidly provide accurate and accessible information to military decision-makers.

(b) This includes the submission of the initial incident report and any updates that result from analysis or response actions taken. It also includes any notification to other CND organizations, HQ, and stakeholders.

(c) Reporting and notification happen throughout the entire cyber incident handling process rather than just one time. As more information is obtained or learned, it is passed on to relevant stakeholders.

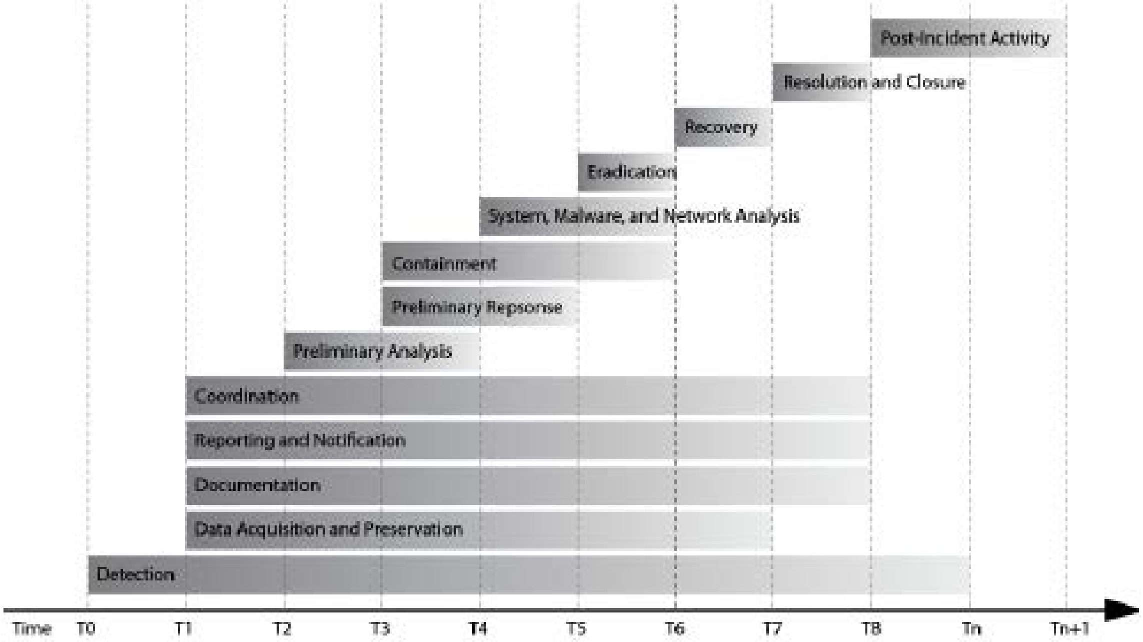


Figure B-2. Relationship of Cyber Incident Handling Phases

(2) Documentation

(a) Documentation is not limited to initial documentation of an incident in an incident reporting form as a submission to the Joint Incident Management System (JIMS). It also includes documentation of additional information gathered during analysis and response. The primary vehicle for reporting and recording all cyber incidents (and reportable events) is JIMS. JIMS replaced the Joint Threat Intelligence Database as the Department of Defense's central repository for this key intelligence.

(b) Any response actions taken may also be part of this documentation, including preliminary response actions, first responder actions, or actions taken to preserve and protect incident artifacts, evidence, or chain of custody.

(3) Coordination. This includes coordination between CC/S/A/FAs and other stakeholders to:

(a) Gather information such as log and artifact collection.

(b) Share information such as situational awareness and intelligence information.

(c) Plan and implement response strategies across affected components.

d. Table B-1 presents the relationship between the ongoing support activities and the basic phases of incident handling.

(1) These activities are part of an iterative process. They are required when there are changes to the status of activities, reportable events, and incidents and continue throughout the incident handling life cycle. The incident handling life cycle shares similar characteristics with a business and military strategy known as the Observe, Orient, Decide, and Act Loop.

(a) Observe. Monitor and detect anomalous or suspicious activity within DoD information networks and ISs.

(b) Orient. Collect, validate, and analyze information available about an incident to characterize the perceived threat and identify, with confidence, the nature, scope, root cause(s), and potential impact of an incident.

(c) Decide. Based on the available information, identify the necessary COA required to contain the incident, eradicate the risk, and recover from the incident.

(d) Act. Execute the COA required to resolve and close the incident and subsequently perform a postmortem. As with military combat, the goal is to be more effective and to execute defensive actions more quickly than the adversary is able to attack. The following sections discuss the incident handling process and activities in more depth. Although they are presented in a logical, sequential order during the life cycle of an incident, they may be done repetitively, in parallel, or sequentially, depending on the requirements of the incident.

	Reporting and Notification	Documentation	Coordination
Detection of Events	Submission of report of events of interest	Initial documentation of event activity	Global information sharing and gathering between tiers and with other CND components, LE/CI, or IC
Preliminary Analysis and Identification	Submission of initial incident report	If no documentation has been started, initial documentation should occur here	Coordination to identify additional sources of information and artifacts
Preliminary Response Action	Update of actions taken	Documentation of any actions taken	Coordination of technical and organizational steps taken to implement preliminary actions across all affected CC/S/A/FAs
Incident Analysis	More detailed updates of analysis performed	Documentation of analysis results	Coordination of incident analysis activities between CND and technical and management components and internal/external subject matter experts
Response and Recovery	Updates on actions taken and submission of final report for closure	Documentation of response plan, analysis performed, and COAs	Coordination of response actions among CC/S/A/FAs, CNDSPs, installations, and CND service subscribers, and with LE/CI, IC, and others as required
Post-Incident Analysis	Submission of Post-Incident Analysis report	Documentation of lessons learned and resulting improvement plan	Coordination between CC/S/A/FAs to implement any process improvement activities resulting from post-incident analysis

Table B-1. Relationship of Cyber Incident Handling Process and Ongoing Supporting Activities

e. Detection of Cyber Events

(1) 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.

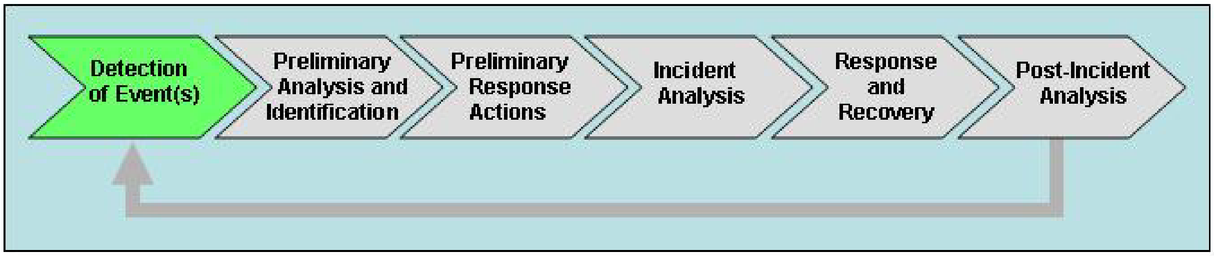


Figure B-3. Detection of Cyber Event(s)

(2) The primary objectives of detecting cyber events include:

(a) 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.

(b) Ensuring suspicious activity is reported in a timely manner consistent with required reporting timelines.

(c) Effectively coordinating with command channels and other DoD organizations.

(3) 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.

(4) Detection starts the reporting process. Gathering report information in a database helps analysts identify emerging trends and patterns. This knowledge can help the CC/S/A/FAs learn from ongoing activity and incidents so they can properly secure and defend their infrastructures.

(5) Detecting Cyber Events

(a) For proper detection to take place, guidelines must be established defining what is abnormal or suspicious. This information must be passed on to appropriate network and IS administrators or incorporated into the configuration of automated detection systems.

(b) Without the detection process, CC/S/A/FAs and CNDSPs would not be alerted that something must be checked or resolved. If this does not happen in a timely, standard, consistent manner, it is possible that a serious incident will not be properly reported, and significant damage and loss to the component infrastructure can occur.

(c) 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.

(d) Cyber incident detection can be from any stakeholder, and initial event detail can vary. Alerts from automated detection systems might include more specific details than a report from a non-technical user. Additional information may need to be collected as part of the incident analysis phase.

(e) Examples of cyber events and the various ways they are detected are provided below.

1. The network intrusion detection sensor sends alerts for suspicious network traffic.

2. The antivirus (AV) software alerts that a device is infected with a worm, virus, or other form of malicious logic.

3. A Web server crashes.

4. Users complain of slow access to hosts on the Internet or mail servers.

5. The IS administrator sees a filename with unusual characters.

6. The user calls the help desk to report a suspicious e-mail message (e.g., phishing).

7. The IS records a suspicious configuration change in its log.

8. The IS logs multiple failed login attempts from an unfamiliar remote IS.

9. The e-mail administrator sees a large number of e-mails with suspicious content.

10. The network administrator notices deviation from typical network traffic flows.

11. The firewall administrator sees unauthorized outbound connections not seen by other means.

(f) An event is not determined to be an incident until some preliminary analysis is done to assess and validate the event against the criteria for determining if it is an incident.

(g) If it is a reportable cyber event or confirmed incident, it is categorized, and the incident handling process should be followed.

(6) Detecting Cyber Events Methodology

(a) Detect cyber event. Identify suspicious behavior or cyber events of interest. A person or an automated system may detect cyber events.

(b) Cyber event detected by a person

1. If a cyber event is witnessed by a user or an administrator, that person must report the information to the designated point of contact (POC). The POC might be a help desk, Information System Security Officer, a CNDSP, or a local IS and network administrator.

2. The report can be submitted by phone, e-mail, reporting form, or some other identified mechanism as identified in Enclosure C or based on the guidance distributed within the affected component. It is important to note that, in most cases, incidents occurring on a classified system are classified. Ensure these types of reports are not reported via unclassified methods.

3. CC/S/A/FAs must ensure that DoD personnel within their area of responsibility (AOR) know what type of activity constitutes an

incident and where and how to submit information about suspicious activity, including reportable cyber events and incidents.

(c) Cyber event detected by an automated system

1. If the cyber event is detected by an automated system, an alert will be sent to the POC designated for receiving such automated alerts.

2. CC/S/A/FAs that maintain automated detection systems and sensors must ensure that a POC for receiving the alerts has been defined and that the IS is configured to send alerts to that POC.

3. The POC must then ensure that the cyber event is reviewed as part of the preliminary analysis phase and reported to the appropriate individuals if it meets the criteria for a reportable cyber event or incident.

(d) Document cyber event information. Present a basic characterization of the activity.

1. If the cyber event is detected by a person, the POC to whom the cyber event is reported or the first responder will collect the symptoms and indicators from the person who noticed or reported the cyber event as the start of documentation.

2. If the cyber event is detected by an automated system, the initial logging and alert will be considered the start of the documentation process.

(e) Coordinate with others

1. Coordinate with the appropriate Tier II CNDSP, command, and technical channels so they are informed of the issue.

2. As appropriate, share or corroborate this information with other CC/S/A/FAs for validation or situational awareness.

f. Preliminary Analysis and Identification of Cyber Incidents

(1) 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 (Figure B-4).

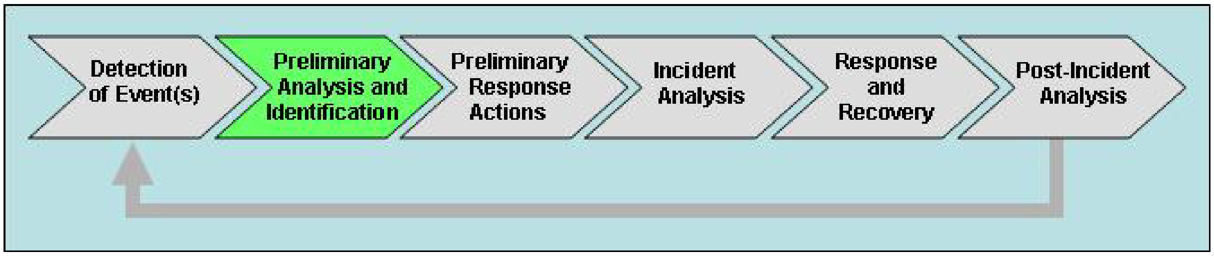


Figure B-4. Preliminary Analysis and Identification of Cyber Incidents

(2) The primary objectives for this phase include the following:

(a) Determining whether a detected event is a reportable cyber event or incident.

(b) Ensuring all appropriate DoD organizations are notified through technical and operational reporting channels.

(c) Ensuring the timely submission of an initial incident report that contains as much complete and useful information as is available (or possible).

(3) 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:

(a) General description of the problem, event, or activity.

(b) Status (ongoing or ended; successful or unsuccessful).

(c) Number of ISs affected.

(d) Source and destination Internet Protocol (IP) addresses.

(e) Source and destination ports.

(f) Hostname(s).

(g) IS location.

(h) User information.

(i) Timestamps.

(j) IDS alert and payload data (if relevant).

(4) Assignment of Category Type

(a) A cyber incident or reportable event category is a collection of events or incidents that share a common underlying cause for which an incident or event is reported. Each cyber event or incident is associated with a category as part of the incident handling process. Cyber incident and reportable event categorization is outlined in Appendix A to Enclosure B (Cyber Incident and Reportable Event Categorization).

(b) 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.

(c) After further investigation, a single cyber event or incident can lead to discovery of additional events. For instance, a network scan (Category 6) of a large number of hosts may be reported. Upon further analysis, it is determined that one of the hosts scanned is also misconfigured (Category 5). This should result in an additional Category 5 report being submitted along with the original Category 6 report. Incident and reportable event categorization is outlined in Appendix A to Enclosure B (Cyber Incident and Reportable Event Categorization).

(5) Preliminary Analysis and Identification Methodology

(a) Assess and Categorize. Assess the event against the incident criteria to determine if it is a reportable cyber event or incident.

1. 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.

2. The security classification of the incident is determined at this stage in accordance with DoDI O-3600.02, “Information Operations (IO) Security Classification Guidance” (reference f), or local CC/S/A/FA original classification authority approved classification guidance.

3. Based on the incident’s category, nature, and impact, determine if the computer forensics process should be initiated.

(b) Perform preliminary impact assessment. Determine the potential damage of the reportable cyber event or incident.

1. This preliminary impact assessment should be conducted in accordance with Appendix C to Enclosure D (Impact Assessment Matrix).

2. 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.

3. 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).

(c) 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.

3. Submit Initial Report. Prepare and submit the initial report to the appropriate organizations and commands and through the appropriate reporting mechanisms.

a. There are two different types of reporting.

(1) Technical Reporting. This technical channel is designed to assist with the handling of incidents and provide fixes to mitigate the operational and/or technical impact of an incident. It may include submitting an incident report to the JIMS, appropriate CNDSP, or any other appropriate reporting channels. Report submission should follow the procedures and formats outlined in the incident reporting procedures in Enclosure C (Cyber Incident Reporting).

(2) Operational Reporting. This channel provides notification to commanders at all levels about the status of their ISs or information networks and the operational impact of the incident on the mission(s). It is a vital conduit for the commanders to identify the operational impact and direct the incident handling process to mitigate unnecessary negative impact on their mission(s).

b. The type of reporting is based on the nature and category of the incident. If appropriate, this is when the LE/CI community should be notified of an incident that may require an investigation IAW DoDI 5505.3, “Initiation of Investigation by Military Criminal Investigative Organizations” (reference g).

c. Incident reports must be submitted to the JIMS by the CNDSP and updated as the status changes. See Appendix A to Enclosure C (Reporting Timelines).

d. Initial incident reporting can include verbal notifications, e-mail summaries, and technical incident reports as appropriate.

e. Incident reporting procedures identified in Enclosure C (Cyber Incident Reporting) will be followed.

f. Timelines for reporting are outlined in Table C-A-1 (Reporting Timelines). Additional guidance on reporting timeframes are provided by command authority OPORDs or other specific guidance.

g. Incidents and reportable events shall be reported at the appropriate classification level using the appropriate means (i.e., Nonsecure 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.

h. 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.

4. 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 (Figure B-5).

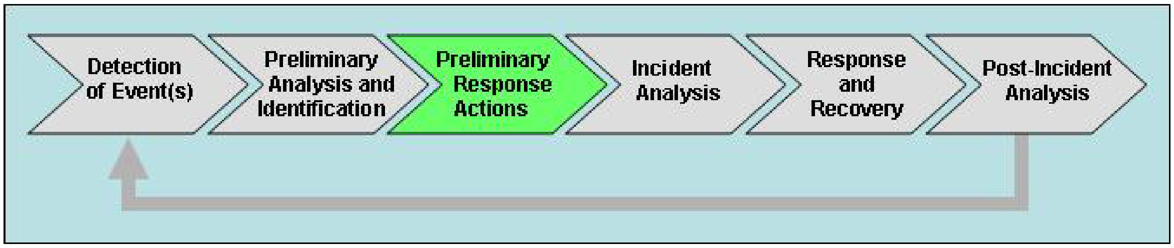


Figure B-5. Preliminary Response Actions

a. Preliminary Response Action Objectives. 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.

b. Preliminary Response Action Methodology

(1) Contain the incident

(a) Contain any potential threat to protect the affected IS or information network and prevent any further contamination, intrusion, or malicious activity.

(b) Containment can be done by an automated detection system or by incident handling staff working in conjunction with technical and management staff.

(c) Containment will be coordinated with the supporting CNDSP. The commander and supporting CNDSP will coordinate with LE/CI as required.

(d) 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.

(2) Acquire and Preserve Data. Safely acquire and preserve the integrity of all data (as directed) to allow for further incident analysis.

(a) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

(3) Continue Documentation

(a) 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.

(b) 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.

4. Cyber Incident Analysis

a. 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 (Figure B-6).

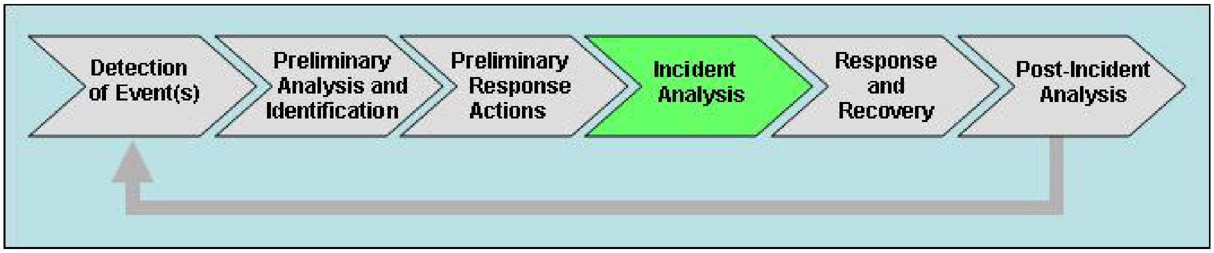


Figure B-6. Cyber Incident Analysis

b. 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.

c. Cyber Incident Analysis Framework. It is important to understand the different types of incident analysis.

(1) 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).

(2) 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.

(3) 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.

(4) See Enclosure D (Cyber Incident Analysis) for additional guidance.

d. Cyber Incident Analysis Methodology

(1) Gather Information. Identify and collect all relevant information about the incident for use in incident analysis.

(a) Information gathered may include data previously acquired and preserved, external logs, personal accounts, all-source intelligence, technical information, or the current operational situation.

(b) Any software artifacts suspected of being malware should be submitted to the Joint Malware Catalog (JMC).[1] Additional guidance may be found in Enclosure G (Computer Network Defense Incident Handling Tools).

(2) Validate the Incident. Review, corroborate, and update (if applicable) the reported incident to ensure all information is accurate as reported.

(a) Reports should be reviewed and updated to maintain situational awareness, to add to incomplete information, or to correct erroneous information contained in the report.

(b) Report validation may require the review of trusted network and system logs or affected ISs to determine if the suspected activities happened as reported.

(c) Verify that the incident is categorized properly, in accordance with Appendix A to Enclosure B (Cyber Incident and Reportable Event Categorization).

(3) 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.

(a) 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.

(b) 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 A to Enclosure D (Delivery Vectors).

(4) 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.

(a) 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.

[1] The JMC is currently under development.

(b) System weakness identification should be performed IAW Appendix B to Enclosure D (Information System Weaknesses).

(5) Identify Root Cause(s). Analyze the information to determine the system-specific cause(s) of the incident.

(a) 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.

(b) 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.

(c) 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.

(6) 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 C to Enclosure D (Impact Assessment Matrix). The impacts to be determined are as follows:

(a) 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. Examples include:

1. Network health status.

2. Potential data compromise or loss.

3. Equipment downtime or destruction.

4. Impact on other ISs or components (e.g., a machine removed from operations takes 8 hours to be rebuilt).

(b) 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.

1. Examples of direct impact include the following:

a. Stolen national intelligence, operational plans, Commander's COP, and decision briefs that provide an adversary with a critical advantage.

b. Corrupted databases (leading to loss of confidence in the intelligence); execution of corrupted/degraded air tasking orders or time-phased force deployment data (TPFDD) leading to loss of mission and/or lives.

c. Hard drive data lost from the DoD networks.

d. Degraded or denied C2 of all networked weapon systems.

e. Degraded, denied, or misdirected C2 from leadership to subordinate units.

f. Loss of control of DoD Supervisory Control and Data Acquisition networks.

2. Examples of indirect impact on a supply organization include the following:

a. An Army division is unable to order/track/process repair parts using a networked IS and is therefore unable to conduct combat operations due to insufficient availability of repair parts.

b. Barges on the Mississippi River are unable to deliver supplies because their crews cannot access DoD-supplied river hazard data.

c. A Reserve unit goes unpaid because of an incident affecting TPFDD, and the unit does not meet its deployment timeline.

(c) TIs are normally reported by the communications and technical component of an organization (J, G, S, N, A-6), while OIs are typically reported by and/or to the operational component of an organization (J, G, S, N, A-3). Examples follow:

1. J-6 reports that an attack accessed 3 megabytes (MB) of data from a server.

2. J-3 reports the attack accessed 3 MB of unclassified family support group data and determines no operational impact.

(d) Determine if the incident has any strategic significance and whether it is a Commander's Critical Information Requirement (CCIR) of USCYBERCOM or other commands and report appropriately.

(7) 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.

(a) 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.

(b) 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.

(c) 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."

(d) Actions that potentially affect traffic on the DoD Protected Traffic List (see Enclosure G) must be coordinated with USCYBERCOM.

(8) 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 deconfliction of operations are crucial to conducting an effective incident response. For additional guidance, refer to Appendix A to Enclosure F (Coordination and Deconfliction).

(a) Coordination ensures that the identification and deconfliction 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.

(9) 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.

(a) Trending Analysis. 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.

(b) Enterprise Threat Fusion and Correlation. This process involves correlating incident activity to assess and direct operation and defense of the DoD information networks across strategic, operational, and tactical boundaries. It includes developing, disseminating, and directing the implementation of countermeasures to specific weaknesses against known adversarial tactics, techniques, and procedures (TTPs) to preserve the Warfighter's ability to carry out current and future missions.

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 (Figure B-7).

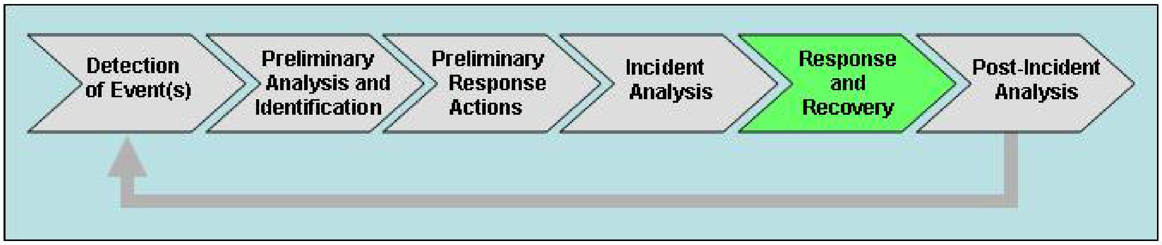


Figure B-7. Response and Recovery

a. 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 C to Enclosure D (Impact Assessment Matrix).

b. Response and recovery may require a combination of technical, management, and/or LE/CI actions.

(1) Technical actions include changes in the network and IS infrastructure to remove the risk or threat.

(2) 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.

c. <u>Response and Recovery Methodology</u>

(1) <u>Implement Containment</u>

(a) Implement (if applicable) additional containment actions to regain control of or isolate the system and prevent further malicious activity.

(b) 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.

(c) 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.

(2) Eradicate Risk. Eradicate the risk and take actions that remove the cause of the incident from the IS/network.

(a) No system should be rebuilt until system data has been adequately preserved and the vulnerability has been mitigated.

(b) ISs having a Category (CAT) 1, 2, and 7 cyber incident 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.

(c) Mission impact may require patching the affected component and instituting temporary vulnerability mitigation until the mission allows the IS to be rebuilt.

(3) 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.

(a) For some incidents, eradication is either not necessary or is performed during recovery.

(b) 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.

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

(5) 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).

(6) 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.

(7) Update Response Actions and Battlefield Damage Assessment (BDA) and Close Incident. Update the incident record in JIMS that closes out the incident.

(a) Ensure all parties have completed the necessary actions for the response.

(b) The BDA documents the technical and operational impact (i.e., OPSEC assessment) of the incident on the organization. It should be determined IAW Appendix C to Enclosure D (Impact Assessment Matrix).

(c) Update the JIMS incident record with the BDA within 24 hours after the incident is resolved.

(d) Declare the incident closed, change the status in the JIMS to closed, and perform any other actions to close the incident.

1. Incidents cannot be closed as a CAT 8—Investigating.

2. An incident might be closed for the CC/S/A/FA or the CNDSP but still remain open for LE/CI investigation.

3. 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.

(8) Additional information about responding to incidents is described in Enclosure E (Cyber Incident Response).

6. Post-Incident Analysis

a. 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 (see Figure B-8).

b. 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.

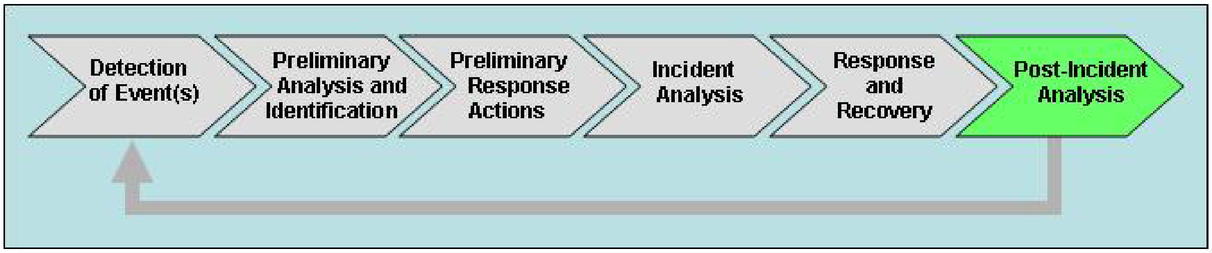


Figure B-8. Post-Incident Analysis

c. 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.

d. CC/S/A/FAs will establish a formal postmortem process and will establish criteria governing which incidents require a postmortem.

e. Not all incidents require a postmortem. Usually, incidents that are large in scope, handled poorly, involved LE, or caused severe damage require a postmortem.

f. Incidents that do require a postmortem will be sent to USCYBERCOM.

7. First Responder Guidelines

a. The first responder is the first person who arrives to investigate and respond to any detected activity. First responders include, but are not limited to, system administrators, CNDSP technical staff, and LE. A first responder's role and responsibilities are to:

(1) Determine the initial impact of the incident.

(2) Collect as much information about the incident as possible.

(3) Document all findings.

(4) Share this collected information with appropriate points of contact to support root cause identification.

b. First responder procedures and processes must be in place to ensure the consistent and proper initial response to events, incidents, or other suspicious activities.

(1) Detectors. People who detect events or incidents must be properly trained to ensure they do not damage or contaminate evidence. They must be taught to step away from the affected or involved IS and to touch nothing; instead, they should report what they have found or seen to the appropriate POC or CNDSP. The POC or CNDSP is responsible for ensuring a qualified person is assigned to handle collection, analysis, and response.

(2) Responders. The people who arrive to investigate and respond to a cyber event or incident are true first responders, just as firefighters or police are the first responders to physical security events. Guidance to these first responders is vital to ensuring proper methods are initiated for appropriate response actions.

(a) First responders must have a defined process and procedure in place governing what they can and cannot do at the scene. First responders who will not handle the investigation or analysis must be ready to turn over all their information in a clear, concise manner that is easily understood by others.

(b) First responders must be knowledgeable and prepared to collect data and forensic evidence. Along with a standard incident response and reporting plan, they must also have a tested and documented toolkit that can be used for collection (data acquisition) and response in a forensically sound manner.

c. Policies and Procedures

(1) Policies and procedures are required to ensure a consistent and proper response to events and incidents that includes:

(a) Determination of a designated first responder and his or her responsibilities. If the first responder will not be the person to handle the incident or does not have the skills or tools needed, the first responder must be carefully instructed to not touch the IS or make any changes and wait to hand over the investigation to the assigned analyst.

(b) Guidance for non-expert or technical personnel who detect a cyber event or incident to ensure they do not make changes to the IS and to ensure they report the event to the appropriate command authority or CNDSP.

(c) Instructions for creating, using, and maintaining a first responder trusted toolkit.

(d) Infrastructure to create and maintain a trusted test bed to test and document tools before adding them to the toolkit.

(e) A defined collection strategy that outlines what type of information and data will be collected, with what tools, and how information and data will be stored and documented.

(f) Instructions for performing forensic data acquisition and maintaining a corresponding chain of custody.

(g) Instructions about what type of preliminary response actions the first responder is approved to make related to containment, notification, or documentation actions.

(2) Each CC/S/A/FA, in coordination with its CNDSP, will define first responder policies and procedures for its areas and provide guidance to Tier III.

d. Precautionary Measures. Prior to the arrival of an authorized incident response analyst, first responders are responsible for taking precautionary measures to ensure the successful acquisition and preservation of data.

(1) Maintain Control. Prevent unauthorized access to the IS and maintain physical control of the surrounding environment. Protect the integrity of other devices that may have witnessed or captured information related to the incident such as log servers, video cameras, remote access

servers, etc. Be aware of unintentional destructive activity such as maintenance procedures that purge and rotate log files, processes that delete files and e-mails after a certain date, etc.

(2) Document Events and Activities. Immediately start a log of activities as soon as a security incident is detected. This log should note when the incident was detected, by whom, and how it was detected. All activities pertaining to the incident should be included in the log, such as opening log files for viewing, printing reports, etc. At a minimum, document the following items:

(a) Time and date of incident.

(b) State of the IS when incident was discovered (on, off, connected, or disconnected).

(c) All activities and commands done to the IS, noting the time, date, and who performed the actions.

(d) People present or knowledgeable about the incident.

(e) Owner or user of the IS.

(3) Determine if Shutdown is Necessary. As soon as it is determined an incident has occurred, the computer should be kept on and in the same state as when the incident was discovered. Guidance for shutting down, altering settings, saving settings, or any other action will be determined by the incident responder (i.e., analyst and LE).

(4) Log Actions. Ensure all actions are logged as part of documenting the chain of evidence.

e. First Responder Toolkits

(1) A first responder toolkit is a set of scripts, programs, and other resources used to safely acquire, examine, and preserve volatile and non-volatile data from an IS.

(2) These trusted toolkits must be approved by the AO, formally known as the DAA, and then must be acquired, described, and fully understood prior to their use.

(3) Information about what the tool does, how it interfaces with an IS and network, what type of outputs it produces, and what type of impact or fingerprint it leaves on the analyzed IS must be determined and documented.

If this is not done or if untested tools are used, then changes may be introduced to the IS that will inhibit a complete analysis, cause a misinterpretation of the activity, or cause the evidence to be contaminated.

(4) First responders must also ensure that any actions they take do not violate any existing CC/S/A/FA computer and network usage policies.

(5) More in-depth information about performing forensic data acquisition and analysis, documenting the analysis and chain of custody, and protecting the collected data is provided in Enclosure D (Cyber Incident Analysis).

APPENDIX A TO ENCLOSURE B

CYBER INCIDENT AND REPORTABLE CYBER EVENT CATEGORIZATION

1. Introduction

a. 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.

b. Each cyber event or incident is associated with one or more categories as part of the incident handling process.

2. Categories

a. In cases where more than one category applies, the category assigned should be determined using the following precedence in Table B-A-1.

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 B-A-1. Category Precedence

b. For instance, an incident could be reported either as a User Level Intrusion (Category 2) or a Non-Compliance Event (Category 5). The User Level Intrusion takes precedence based on Table B-A-1, and the incident should be reported as a User Level Intrusion (Category 2) incident.

c. Investigating (Category 8) reports will include an initial assessed incident category (Categories 1-7 or 9) and be recategorized based on continued investigation. No reports will be closed as a Category 8.

d. Table B-A-2 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 is defeated/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 recategorized 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 B-A-2. Cyber Incident and Reportable Cyber Event Categories

3. Comparison of DoD and Department of Homeland Security Categories. Table B-A-3 provides a comparison between categories utilized by the Department of Defense and Department of Homeland Security (DHS).

DoD Cyber Incident and Reportable Cyber Event Categories	DHS Incident and Reportable Event Categories
Category 0: Training and Exercises	Category 0: Exercise/Network Defense Testing
Category 1: Root-Level Intrusions	Category 1: Unauthorized Access
Category 2: User-Level Intrusions	Category 1: Unauthorized Access
Category 3: Unsuccessful Activity Attempt	Category 5: Scans/Probes/Attempted Access
Category 4: Denial of Service	Category 2: Denial of Service
Category 5: Non-Compliance Activity	Category 4: Improper Usage
Category 6: Reconnaissance	Category 5: Scans/Probes/Attempted Access
Category 7: Malicious Code	Category 3: Malicious Code
Category 8: Investigating	Category 6: Investigation
Category 9: Explained Anomaly	

Table B-A-3. Comparison of DoD and DHS Incident and Event Categories[2]

[2] The eventual goal is to coordinate common incident and event categories between the Department of Defense and DHS.

ENCLOSURE C

CYBER INCIDENT REPORTING

1. Introduction

a. 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.

b. Reporting provides valuable input into the combined and coordinated analysis of data from a variety of sources.

(1) This analysis provides the joint forces, CC/S/A/FA CNDSPs, and USCYBERCOM with indications of adversary reconnaissance, probing, intrusions, network exploitations, and/or attacks that have occurred or are occurring on DoD information networks.

(2) It also enables regional and theater entities to understand what is happening across their joint/theater operations, and, in turn, provides information to Tier Is, which are able to gain a global situational awareness of attacks occurring on DoD information networks.

c. This section provides guidance on the reporting requirements for reportable cyber events and incidents.

(1) Further requirements shall be articulated in OPORDs issued by relevant commands.

(2) DoD, contractor, or other personnel who access DoD ISs and information networks must report to their appropriate organization and commands (whether that is a supervisor, information assurance manager, information assurance officer, commander, CNDSP, etc.).

d. The primary objectives for the incident reporting process are to:

(1) Ensure all suspicious activity on DoD information networks and ISs is reported according to defined policies, procedures, and within established timeframes.

(2) Ensure incident reports provide an accurate, meaningful, and complete understanding of the incident throughout its life cycle.

(3) Ensure the effective and timely coordination and communication of incident information through appropriate channels and with higher CND organizations and/or DoD CC/S/A/FA HQ.

(4) Provide the Department of Defense with the ability to direct protective and defensive strategies based on incident reporting trends and adversarial activity.

e. Events and incidents are reported and communicated across multiple tiers within the Department of Defense, including the Joint Staff, CC/S/A/FAs, CNDSPs, and the installations at Tier III levels. Each tier plays a role in this incident reporting process to support situational awareness and operational impact reporting about activities that affect CC/S/A/FAs. Such reporting serves multiple purposes and serves different needs within the Department of Defense, for example:

(1) Initial detection and notification alert appropriate organizations that activity has occurred (or is occurring) that requires attention.

(2) Follow-up notification provides further details and updates regarding status or changes in the **activity** to support ongoing analysis, remediation, or development of response COAs.

(3) Accurate and complete information gives analysts data used to assess the impact of an incident and the impact it has on mission operations.

(4) Accurate and complete reporting assists analysts in determining root cause(s), in identifying delivery vectors, and/or identifying IS weaknesses.

(5) Accurate and complete reporting provides relevant input to the intelligence community and supports LE/CI investigations.

(6) Timely reporting provides input to Tier I to enable a DoD-wide understanding of the current defensive operational picture.

(7) Comprehensive incident reporting provides data that can be used in other correlation, trending, or retrospective analysis tasks.

(8) Increased knowledge and awareness can help keep other incidents from happening or going undetected.

f. Effective end-to-end reporting serves as input to the defensive operational picture, which provides local, intermediate, and DoD-wide visual situational awareness of incidents, events, CNDSP actions, and their impact. To accurately identify, characterize, and understand activity occurring across DoD information networks, commanders at all levels must ensure their subordinates participate in the reporting process.

g. There are requirements and benefits across all tiers from appropriately sharing information about incident reports. For example, activity identified at a Tier II entity that is reported up to Tier I and pushed down to Tier III can additionally be passed on to peer CC/S/A/FAs to alert them to similar activity. Sharing information about an incident at one location with peer organizations can facilitate improvements or enable peer entities to protect their ISs and DoD information networks proactively.[3]

2. Reporting Structures

a. Effective response requires coordinated reporting and information sharing with multiple communities of interest within and outside the Department of Defense. 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.

b. Technical Reporting Structure

(1) All reportable events and incidents are reported to USCYBERCOM. Defined processes and procedures will be followed at each tier to ensure reportable incidents and events contain relevant information IAW this manual to enable the Department of Defense to appropriately handle those incidents and events, as well as to gain an in-depth view of activity and any operational impact on DoD mission operations.

(2) The level and type of information to be reported will depend on the operational roles and responsibilities of the individuals involved, as well as any specific OPORDs. When incidents and reportable events are identified, it

[3] Online collaborative tools provide a proven environment to conduct these information sharing activities. Persistent sessions between tier entities can be established to track and collaborate on ongoing incidents and events.

should be recognized that reporting occurs through a management channel as well as a technical channel. These channels are described below:

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

1. Technical activities include reporting incidents and events through appropriate channels, updating information throughout the life cycle of the cyber event or incident, and conducting other communications related to them.

2. The dissemination of information and types of communications will vary depending on the roles involved in the activity (Tier I, II, or III; LE/CI; joint commands; etc.).

(b) Operational Reporting. The management and oversight channel is designed to notify commanders at all levels of the ability of their ISs to support operations and the operational impact of any reported incidents.

1. Commanders determine when to initiate communications with the LE/CI community, for example, when an incident requires a criminal investigation.

2. The type of reporting will also depend on the leadership role involved in the notification path (e.g., communicating with control centers, CNDSPs, USCYBERCOM, LE/CI, or the IC).

3. The leadership and oversight channel also provides a conduit for commanders to guide the incident handling process to mitigate any additional negative impact on their ISs.

(c) These technical and operational reporting channels occur in parallel. They ensure that incidents and their potential impact are addressed not only at the technical (detection, analysis, and response) levels, but that commanders and other appropriate DoD personnel receive details to enable appropriate tactical and strategic military decision making. Commanders are ultimately responsible and accountable for their information networks and for ensuring that appropriate reporting occurs.

(3) 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.

(a) Incidents are reported to USCYBERCOM according to published CCIRs.

(b) USCYBERCOM provides reports (summaries, significant incidents, trends, enterprise-wide issues) to OSD through USSTRATCOM and the Joint Staff as required.

(c) USCYBERCOM receives reports of all reportable events and incidents from Tier II (CNDSP) through the JIMS.

(d) USCYBERCOM analyzes, correlates, and fuses reports to understand attacks against DoD information networks and to direct defensive measures. This information, in turn, is shared (as appropriate) with other tiers.

(e) USCYBERCOM disseminates information to the USSTRATCOM Joint Intelligence Center (STRATJIC) about DoD Enterprise Incident Sets.

(f) USCYBERCOM coordinates with LE/CI regarding incidents that involve LE/CI investigations.

(g) USCYBERCOM provides tactical and strategic information to subordinate tiers based on the results of report trending analysis and the correlation and enterprise fusion of threat information. This information is provided in a variety of reports including, but not limited to:

1. Operation orders (e.g., OPORDs, WARNORDs, TASKORDs)

2. Situational awareness reports, bulletins, and alerts

3. Web portals, e-mails, and Defense Connect Online sessions

(h) USCYBERCOM provides releasable incident reporting material to bilateral and multilateral partners as appropriate.

(i) USCYBERCOM J-2 and the Service Component CERT/computer incident response team (CIRT) intelligence support elements are required to perform IAW Appendix B to Enclosure F (Intelligence Support to Incident Reporting).

(j) The LE/CI organizations (at USCYBERCOM) receive reports of incidents that may support LE/CI actions.

(k) The LE/CI organizations (at USCYBERCOM) coordinate the release of CND LE/CI information, with appropriate release authority, from originating agencies to support information sharing across the CC/S/A/FAs.

(l) The NTOC provides AS&W and a variety of technical alerts to USCYBERCOM that are shared (as appropriate) with other tiers to direct response actions.

(4) 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 IAW Appendix A to Enclosure B (Cyber Incident and Reportable Cyber Event Categorization). 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 II entities include:

(a) CND Service Providers (CNDSPs)

1. CNDSPs report incidents within their subscriber community to USCYBERCOM through the JIMS.

2. CNDSPs share valuable information about incidents being reported (if applicable) with other peer organizations.

3. CNDSPs provide feedback to reporting organizations as information is developed. Subordinate echelons in the reporting chain are responsible for relaying information to the originating point and developing procedures to disseminate the information, as appropriate, within their constituent communities (e.g., Network Operations Security Center (NOSC), Theater Network Control Center (TNCC), or Global Network Control Center (GNCC) within the CC/S/A/FA and/or DISA NetOps Center (DNC) within its AOR).

(b) Theater NetOps Center

1. Incidents are reported from the joint HQ or activity to its Tier II CNDSP, the Regional C4I Control Center (CCC)/TNCs, and the Combatant Command HQ.

2. Reports are submitted from the CCC/TNCs to the Joint Staff National Military Command Center as appropriate. CCC/TNCs and Combatant Command HQ report information about events and incidents to Tier I.

3. The TNCs issue technical and operational directives to Service theater NOSCs and agency theater NOSCs.

(c) Service or Defense Agency Network Operations Security Center

1. Each Service and Defense agency NOSC providing CND services to a Service or Defense agency component supporting a regional Combatant Command makes available warnings, reports, information, data, and statistics pertinent to the protection of resources assigned to the regional Combatant Command.

2. Service and Defense agency NOSCs coordinate and report network deception systems to their Tier II CNDSP and USCYBERCOM, for awareness and correlation purposes, prior to connection to any DoD information network. In addition, for situation awareness purposes, they report network deception system deployments (e.g., honey pots) within Combatant Command Service components to that Combatant Command.

3. Service and Defense agency NOSCs report information to USCYBERCOM through their Tier II CNDSP for inclusion into the DoD Protected Traffic List.

4. Service and Defense agency elements subordinate to a Combatant Commander (geographic and/or functional) simultaneously report to a Combatant Command NetOps organization and to their Service or Defense agency NOSC or DNC. Reporting should be accomplished IAW Combatant Command guidance.

(d) Combatant Command HQ. Joint HQ or Regional CCC/TNCs must forward, or make available through the JIMS, information about events and incidents reported to them from the affected components to CC HQ. This helps CC HQ maintain an accurate operational view in its AOR.

(e) Global NetOps Control Center

1. GNCCs receive informational reports from Service elements and Global NetOps Support Centers (GNSCs).

2. GNCCs disseminate CNDSP feedback within the constituent communities as appropriate.

3. GNCCs provide recommendations and advise senior leadership on COAs as appropriate.

(f) Global NetOps Support Center

1. GNSCs report incidents through defined channels (e.g., CNDSP) or as directed by command instructions or policy.

2. GNSCs issue technical and operational directives to Service theater NOSCs and agency theater NOSCs.

(g) Theater Network Control Center

1. TNCCs receive informational reports from Service elements and TNCs.

2. TNCCs provide recommendations and advise senior leadership on COAs as appropriate.

(h) Theater C4I Control Center (TCCC)

1. TCCCs receive informational reports from Service elements and TNCs.

2. TCCCs provide recommendations and advise senior leadership on COAs as appropriate.

(i) CC/S/A/FAs. Incidents (or reportable events) that occur within their subordinate levels regardless of classification are reported to the appropriate CNDSP.

(5) 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). Tier III entities include:

(a) Base/Post/Camp/Stations (B/P/C/Ss). B/P/C/Ss represent the lowest level in which reportable events and incidents occur and from which they must be reported.

1. Service elements at B/P/C/Ss report through Service-defined channels to the Service or agency NOSC, or their CNDSP, which report to USCYBERCOM.

2. Service elements subordinate to a commander of a Combatant Command simultaneously report to a Combatant Command GNCC and a TNCC, as directed by Combatant Command instructions or policy.

3. Joint activities report incidents to their host command NSC, Combatant Command, and TNC.

(b) Network Service Centers. NSCs serve as focal points for reporting and handling incidents and network management at the lowest level.

c. Additional Reporting Structures. Additional reporting structures exist in order to support the IC, LE, CI, and other operational reporting requirements.

(1) Operational Report (OPREPs)

(a) 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.

(b) 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.

1. Root Level Intrusion (Category 1). Unauthorized privileged access to MAC I or MAC II IS(s).

2. User Level Intrusion (Category 2). Unauthorized non-privileged access to MAC I or MAC II IS(s).

3. Denial of Service (Category 4). Denial of Service (DoS) against MAC I or MAC II IS(s).

4. Malicious Logic (Category 7). Active propagation of malware infecting an IS or malicious code adversely affecting the operations and/or security of an IS. OPREPs for previously reported outbreaks are not submitted (e.g., outbreak of virus reported 2 months ago).

(c) OPREP-3 reports will be submitted as soon as possible after cyber incidents have been detected. Speed takes priority over detail.

(d) OPREP-3 initial reports will contain only as much of the requested information as is immediately available. The initial report must not be delayed to gain additional information.

(e) USCYBERCOM submits OPREP-3 for DoD-wide computer network incidents to USSTRATCOM.

(2) Law Enforcement and Counterintelligence Reporting Structure

(a) 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.

(b) 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.

1. Commanders request investigations and the servicing LE/CI organization determines if investigations are to be opened IAW DoDI 5505.3 (reference g).

2. 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.

3. The investigative community has substantial authority to access official government and private sector information, consistent with normal investigative procedures. Ideally, the operational community should cooperate with the servicing LE/CI organization, which will in turn coordinate with LE/CI organizations (at USCYBERCOM). The LE/CI organizations disseminate information to other LE/CI organizations, including non-DoD LE/CI organizations if appropriate.

4. Reporting incidents through LE/CI channels does **not** eliminate the requirement to report incidents through standard technical and operational reporting channels.

5. LE/CI matters and investigations regarding sensitive compartmented information (SCI) networks, ISs, and cleared SCI personnel will be forwarded to SCI LE/CI authorities.

(3) 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.

(a) DoD SCI organizations will provide reporting directly to the DIA Information Assurance Protection Center (IAPC).

(b) Member organizations operating under the authority of the NSA, NRO, and NGA shall report to their agency authority IAW internal agency policy.

(c) DoD IC members will report all reportable events directly to the IC-IRC within established reporting timelines.

1. The IC-IRC will ensure all TS/SCI reports are reported to USCYBERCOM to ensure information about new vulnerabilities, exploits, or incidents reported on compartmented ISs is disseminated to the appropriate IC member organization for remediation.

2. All requests for DoD SCI information will be vetted through the IC-IRC to the responsible community member organization.

3. Additional guidance on phased reporting procedures for intelligence reporting can be found in Appendix B to Enclosure F (Intelligence Support to Cyber Incident Reporting).

3. Operational Reporting Practices

a. Incident reporting plays an essential role in understanding how and when DoD information networks and ISs are being attacked. Achieving this understanding requires a disciplined reporting framework, and individuals responsible for incident reporting are expected to follow some general best practices as part of this process.

b. Critical success factors for incident reporting include the following:

(1) Timeliness. Reporting incidents aids in identifying, characterizing, and responding to adversarial activity. The Department of Defense's ability to respond effectively while minimizing damage is highly dependent on the length of time between when activity is detected and when it is first reported. Reporting incidents in a timely manner accelerates the Department of Defense's ability to develop and implement defensive measures.

(2) Quality and Completeness. An incident report's value is determined by the quality of the information. The more useful information contained in the report, the better it can help analysts understand the technical details, root cause(s), and potential impact of the incident. Incident reports should be regularly updated with as much useful information as is available at the time.

(3) Enterprise-Wide Visibility of Reporting. All incident reports shall be submitted to the JIMS. The consistent, complete, and timely reporting of incident data into a single database is necessary in order to reflect the collective reporting of adversarial activity and can help shape tactical, strategic, and military strategies for response. This information can then later be used to perform trending analysis, correlation, and fusion.

(4) Operational Effectiveness. Incident reports should be managed effectively from creation to resolution. This management is an ongoing and iterative process. Once an incident is reported, it should be updated when its status changes and until the incident is resolved. This allows commanders and others responsible for directing incident response strategies to remain informed about the status of their ISs or DoD information networks and the impact of the incident on their missions. Timely updates and the effective sharing of relevant incident information can also help other DoD organizations recognize the activity and mitigate any negative impact on their mission(s).

c. Organizations at all levels report changes in the status of reportable events, incidents, and incident handling actions. There are a variety of reasons why status reports are issued to the appropriate organizations. Some reasons may include, but are not limited to:

(1) Changes in the characteristics of the reportable cyber event or incident activity.

(a) Increase or decrease in activity.

(b) Operational impact(s) on an IS, DoD information network, or mission.

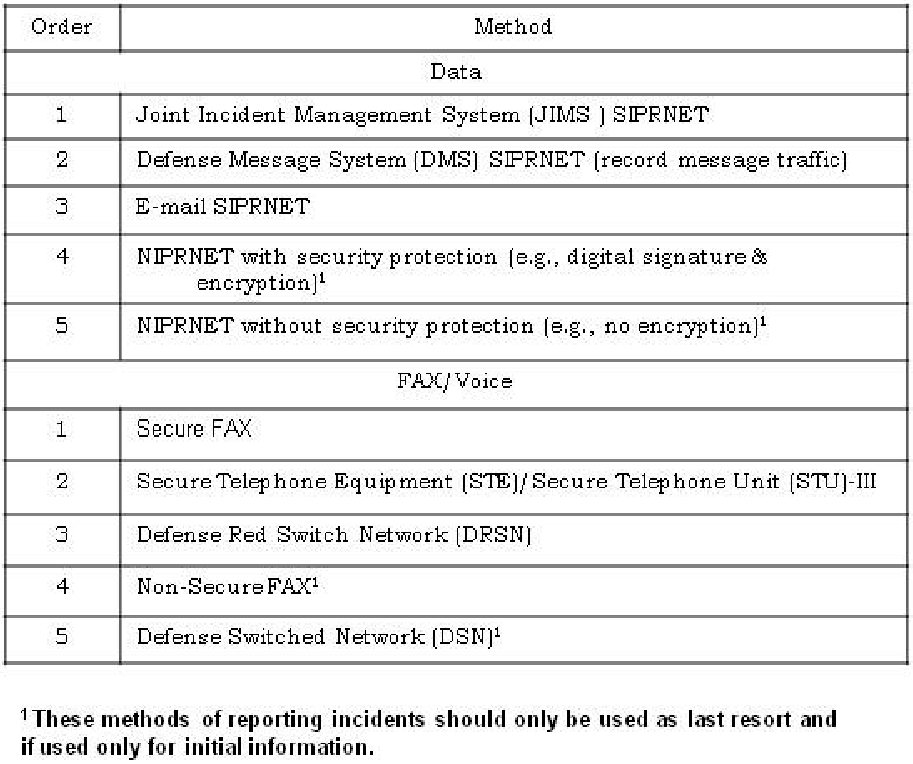
(2) Corrective actions that change the status of the reportable cyber event or incident activity.

(3) Closure of a reportable cyber event or incident.

4. Reporting Vehicles

a. All reportable events and incidents must be reported in a timely manner through approved reporting mechanisms. The primary vehicle for reporting incidents (and reportable events) is the JIMS. Other mechanisms are available, but the JIMS maintains the canonical records for all incident reports.

b. Table C-1 (Reporting Vehicles) 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 & encryption)[1]
5	NIPRNET without security protection (e.g., no encryption)[1]
FAX/Voice	
1	Secure FAX
2	Secure Telephone Equipment (STE)/Secure Telephone Unit (STU)-III
3	Defense Red Switch Network (DRSN)
4	Non-Secure FAX[1]
5	Defense Switched Network (DSN)[1]

[1] These methods of reporting incidents should only be used as last resort and if used only for initial information.

Table C-1. Reporting Vehicles

c. The principal reporting vehicle for DoD SCI ISs is a Joint Worldwide Intelligence Communications System (JWICS) e-mail to the IAPC at iapc@dia.ic.gov. Reporting instructions and format can be found at http://www.dia.ic.gov/admin/ds/iapc at the “DIA Incident Reporting Form.”

d. Submit reports using the most protected means available for the affected IS.

(1) Use SIPRNET or secure phone/fax if those ISs are available.

(2) Unclassified reporting vehicles (NIPRNET, non-secure fax) should only be used for incidents on unclassified ISs.

(3) USCYBERCOM will work with NOSCs, TNCs, and GNCCs/TNCCs/ Tier II CNDSPs to correlate and deconflict incident reporting information.

(4) If necessary, potentially compromised assets will be removed from the DoD information network prior to reporting an incident.

e. Reporting will be done on a DoD information network other than the potentially compromised IS to remove the possibility of an attacker monitoring the compromised DoD information network and potentially intercepting the incident report.

5. Reporting Timelines

a. The reporting timelines establish the minimum requirements and timeframes for which incidents will be reported. They are designed to expedite reporting of incidents where national-level coordination and action may serve to mitigate or prevent damage to DoD information networks.

b. All incidents will be reported IAW the requirements and timeframes defined in Appendix A to Enclosure C (Reporting Timelines).

c. These requirements will not preclude the rapid reporting of any cyber event or incident deemed necessary by the responsible CNDSP or CCIR and do not supersede any requirements established by USCYBERCOM CND CCIRs. These CCIRs may be found on USCYBERCOM's Web site at https://www.cybercom.smil.mil/J3/orders/default.aspx.

d. Additionally, as noted in Appendix A to Enclosure C (Reporting Timelines), some incidents are also reportable using OPREP-3 reporting procedures and structure IAW CJCSM 3150.03, "Joint Reporting Structure Event and Incident Reports" (reference i).

6. Reporting Formats

a. The preferred method for reporting incidents is through the JIMS. The JIMS provides a structured format to conveniently record and submit information about the reportable cyber event or incident to a central database maintained by USCYBERCOM.

b. JIMS Report Format. The JIMS reporting format is used by Tier II CNDSP[4] to report incidents to the USCYBERCOM. It is the primary reporting format and mechanism for submitting reports.

[4] Tier II CNDSPs are responsible for ensuring incidents and events are reported in JIMS. However, CC/S/A/FAs, in conjunction with their Tier II CNDSP, may authorize their Tier III organizations to also report incidents in JIMS.

c. General Report Format

(1) This format is used to report incidents and reportable events from Tier III entities to the respective Tier II CNDSP. CNDSPs are then responsible for submitting these reports into the JIMS.

(2) Appendix B to Enclosure C (General Cyber Incident Report Format) lists the types of information that will be provided.

(3) The format provides a structure for initially reporting incidents and reportable events by JIMS, telephonically, by secure fax, or by other electronic means.

(4) On initial discovery of an incident, not all information will be known; however, as much information as possible should be provided, regardless of the means used to report. Over time, as additional information is identified, follow-on reporting shall be made to complete the form.

(5) Information provided in this format is then used to submit an incident to the JIMS.

(6) CC/S/A/FAs may append more information to the report format to require further information for internal analysis or uses.

(7) As more information becomes available, provide additional details as updates to the initial report in follow-on incident and reportable event reporting.

(8) In order for a report to be considered "complete," it must contain, at a minimum, the information listed in Appendix B to Enclosure C (General Cyber Incident Report Format).

7. Reporting Considerations

a. In addition to the reporting requirements already described, there are several other factors to consider when reporting incidents, to include classification level and whether or not they involve personally identifiable information (PII). Both will have an effect and impose additional requirements on the reporting, including the timeframes and methods.

b. Loss or Suspected Loss of Personally Identifiable Information (PII) Data

(1) PII is any information about an individual maintained by a DoD entity, including, but not limited to, education, financial transactions, medical history, and criminal or employment history. It also includes information that can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information linked or linkable to an individual.

(2) Incidents[5] that also involve loss or suspected loss of PII data require CC/S/A/FAs to augment their processes to report this activity separately IAW DoD 5400.11-R, "Department of Defense Privacy Program" (reference j).

(3) The Department of Defense has established guidance to protect PII. This is mandated through legal, federal and DoD guidance to include FISMA (reference a), OMB Circular A-130 (reference b), DoD 5400.11 (reference j), the Privacy Act of 1974 (reference k), and OMB memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (reference l). CC/S/A/FAs must ensure that PII not explicitly cleared for public release is protected IAW DoD policy. This includes meeting or exceeding requirements described in OMB memorandum M-06-16, "Protection of Sensitive Agency Information (reference m) and OMB memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments" (reference n).

(4) The policy applies to any DoD-owned or controlled ISs or services, regardless of classification or sensitivity, that receive, process, store, display or transmit DoD information.

(5) Loss or suspected loss of PII shall be reported as follows:

(a) Reports must be submitted to the US-CERT within 1 hour of the incident. Loss of PII information on DoD or IC information networks must also be reported to US-CERT within 1 hour of the incident.

[5] Incidents or events (e.g., CAT 1, 2, or 5) could involve the loss of PII and require additional reporting requirements.

(b) Reports must be submitted to the CC/S/A/FA Privacy Office POC within 24 hours. The POC then reports to the DoD Privacy Office within 48 hours or as established by the Defense Senior Privacy Official.

(6) Criteria for determining the risk include:

(a) Will the breach cause harm?

(b) What is the risk level?

(c) How many individuals are affected?

(d) Is the information accessible and usable?

(7) Failing to protect PII can result in civil penalties against DoD components and criminal penalties against individuals.

c. Classification Level. The security classification of an incident is determined IAW DoDI O-3600.02 (reference f). Incident reports will be protected based on their classification and sensitivity. All incidents occurring on the SIPRNET shall be classified at least Secret. Incident classifications higher than Secret depend on the classification level of the material involved (e.g., Top Secret or compartmented), overall impact, and compromise potential. Incidents occurring on NIPRNET ISs will be unclassified and marked Controlled Unclassified Information (CUI) unless exploitation of information in the report by an adversary would result in a classified information compromise or significant negative impact on a national security mission.

8. Exercise Reporting

a. Incident and event categorization and reporting will be IAW this manual.

b. USCYBERCOM will provide separate guidance on identifying exercise incidents/events reported in the JIMS and the processes for deconflicting real-world and exercise activities.

APPENDIX A TO ENCLOSURE C

REPORTING TIMELINES

1. Introduction

a. 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.

b. Included below are definitions for the reporting timelines columns:

(1) Impact. The degree to which an incident or event adversely impacts, or has the potential to impact, the successful accomplishment of operational missions and the confidentiality, integrity, or availability of DoD information networks and ISs. Impact helps characterize the estimated damage or loss resulting from the incident and contributes to the collective understanding of the DoD-wide security posture. Additional information is available in Appendix C to Enclosure D (Impact Assessment Matrix).

(2) Initial Notification to Next Tier. The required notification timeframe between the discovery or awareness of an incident or event and the initial notification to the designated upstream tier. Initial notification serves to provide preliminary information that an incident or event has occurred to those responsible for directing response actions within organizations and commands.

(3) Initial Report to Next Tier. The required reporting timeframes between the discovery or awareness of an incident or event and the initial electronic submission of a report such that it is available to the upstream tier. Initial reports serve to provide details about the incident or event and contain preliminary analysis to characterize the potential technical and organizational implications. Initial reports are updated throughout the life cycle as further analysis and information become available.

(4) Initial Submission to JIMS. The required reporting timeframe between the discovery and awareness of an incident or event and the initial entry into the JIMS such that it is available to the upstream tier(s). The JIMS is the central catalog for managing event and incident reports. Consistent and comprehensive reporting is required in order to accurately characterize the threat environment and security posture of DoD information networks such that a strategic and tactical COA may be developed and implemented.

(5) Minimum Reporting. This defines the lowest tier for which an incident or event will be reported. The minimum reporting requirement can be changed by USCYBERCOM direction.

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 Non-Compliance 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

Table C-A-1. Reporting Timelines

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]	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 C-A-1. Reporting Timelines (continued)

2. Reporting Timelines

a. Reporting timelines will be based on the current and potential impact of the incident or event on the confidentiality, availability, and integrity of organizational operations, organizational assets, or individuals.

b. Additionally, abbreviated reporting timelines give the CNDSP more time to collect, process, and correlate information concerning reportable events and incidents before reporting them at the national level.

c. Follow-on reports are submitted as directed by the higher CND organizations or headquarters.

(1) If no direction is provided, follow-on reports are submitted within 8 hours of the discovery of new information about the incident.

(2) Follow-on reports provide the raw details needed for the regional or global teams to understand the technical nature of the problem and is merged with information obtained from other reports to highlight regional or global trends.

(3) This report is forwarded IAW Table C-1 (Reporting Vehicles).

[6] Acknowledgement from the asset owner that it is investigating the issue.

d. USCYBERCOM provides feedback to reporting organizations as more information becomes known. Subordinate layers in the reporting channels are responsible for relaying this information to the originating point and developing procedures to disseminate the information as appropriate within their constituent communities (NOSCs, TNCC, or GNCC within the CC/S/A/FAs and/or TNC within their AOR). The format is also used by NOSCs or Combatant Command TNCCs and GNCCs and/or TNC organizations to report information developed through observation, correlation, analysis, or other means.

APPENDIX B TO ENCLOSURE C

GENERAL CYBER INCIDENT REPORT FORMAT

1. General Cyber Incident Report Format. Table C-B-1 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.

Table C-B-1. General Cyber Incident Report Format

Field	**Description**
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 disposition of mediums and logs.

Table C-B-1. General Cyber Incident Report Format (continued)

Field	Description
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).

Table C-B-1. General Cyber Incident Report Format (continued)

Field	**Description**
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.

Table C-B-1. General Cyber Incident Report Format (continued)

Field	Description
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 C-B-1. General Cyber Incident Report Format (continued)

2. Initial Impact Assessment Matrix. The System Impact Matrix that follows may be used to provide an initial impact assessment when submitting a report. Initial assessment should be performed quickly even with limited details and analysis. This table calculates impact based on the type of device affected and the incident category. It should only be used during the initial reporting process. The more complete impact assessment conducted later in the incident handling process is done IAW Appendix C to Enclosure D (Impact Assessment Matrix).

	Cyber Incident and Reportable Cyber Event Category						
Network Device	CAT 1	CAT 2	CAT 3	CAT 4	CAT 5	CAT 6	CAT 7
Backbone	High	High	Low	High	Low	Low	Low
Router	High	High	Low	High	Moderate	Low	Low
Network Management / Security Server	High	High	Low	High	Moderate	Low	Moderate
Non-Public Server	Moderate	Moderate	Low	Moderate	Moderate	Low	Moderate
Public Server	Low	Low	Low	Moderate	Low	Low	Moderate
Workstation	Low	Low	Low	Moderate	Low	Low	Moderate

Table C-B-2. Initial Impact Assessment

APPENDIX C TO ENCLOSURE C

CYBER INCIDENT REPORTING DIAGRAMS

1. High-Level Overview of Reporting. The following reporting scenario depicts the general DoD-wide process for reporting incidents, exchanging information, and providing feedback to the DoD community.

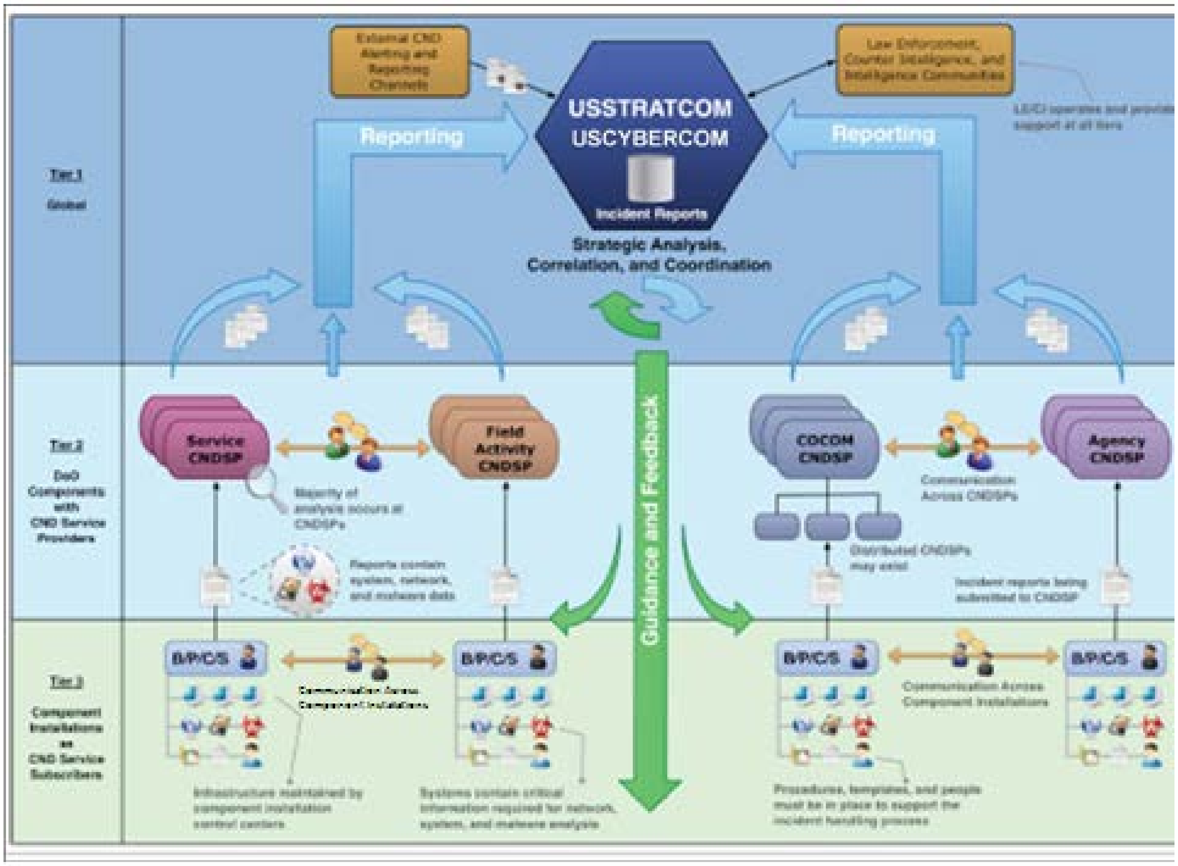

External CND Alerting and Reporting Channels
USSTRATCOM
USCYBERCOM
Incident Reports
Strategic Analysis, Correlation, and Coordination
Law Enforcement, Counter Intelligence, and Intelligence Communities
LE/CI operates and provid support at all tiers
Reporting
Reporting
Tier 1
Global
Tier 2
DoD Components with CND Service Providers
Tier 3
Component Installations as CND Service Subscribers
Service CNDSP
Field Activity CNDSP
COCOM CNDSP
Agency CNDSP
Majority of analysis occurs at CNDSPs
Reports contain system, network, and malware data
Communication Across CNDSPs
Distributed CNDSPs may exist
Incident reports being submitted to CNDSP
Guidance and Feedback
B/P/C/S
B/P/C/S
B/P/C/S
B/P/C/S
Communication Across Component Installations
Communication Across Component Installations
Infrastructure maintained by component installation control centers
Systems contain critical information required for network, system, and malware analysis
Procedures, templates, and people must be in place to support the incident handling process

Figure C-C-1. High-Level Overview of Reporting

2. Cyber Event Detected by Installation. The following reporting scenario depicts the general process for how incidents detected at a DoD installation (e.g., B/P/C/S) are reported. The actions outlined in process may occur simultaneously following the initial detection of an anomalous activity.

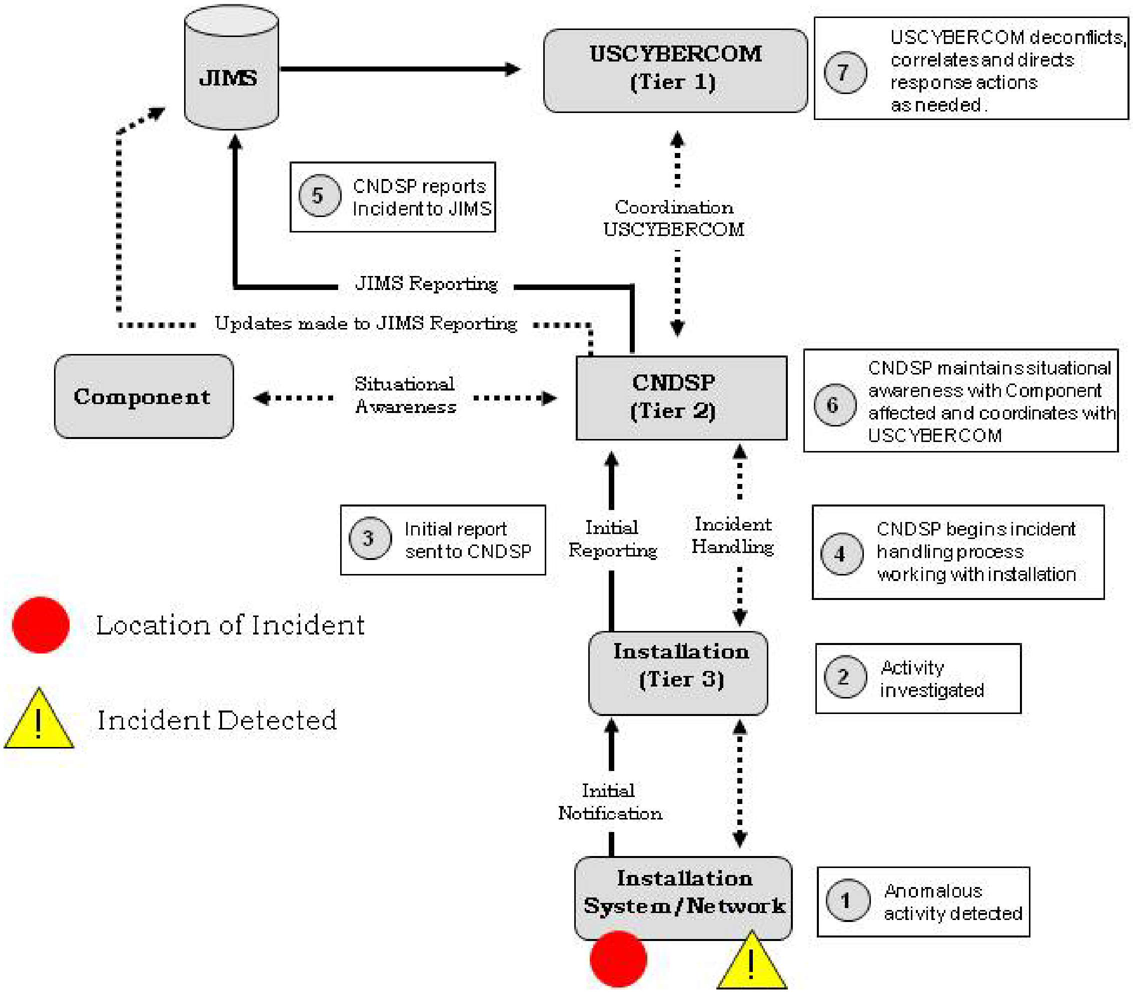

JIMS
USCYBERCOM (Tier 1)
7 USCYBERCOM deconflicts, correlates and directs response actions as needed.
5 CNDSP reports Incident to JIMS
Coordination USCYBERCOM
JIMS Reporting
Updates made to JIMS Reporting
Component
Situational Awareness
CNDSP (Tier 2)
6 CNDSP maintains situational awareness with Component affected and coordinates with USCYBERCOM
3 Initial report sent to CNDSP
Initial Reporting
Incident Handling
4 CNDSP begins incident handling process working with installation
Location of Incident
Incident Detected
Installation (Tier 3)
2 Activity investigated
Initial Notification
Installation System/Network
1 Anomalous activity detected

Figure C-C-2. Cyber Event Detected by Installation

3. Cyber Event Detected Within Combatant Command. The following reporting scenario depicts the general process for how incidents detected within a Combatant Command are reported. One of the key elements in this scenario is that the Combatant Command HQ is provided DoD data necessary to maintain situational awareness to exercise command and control authority within its AOR.

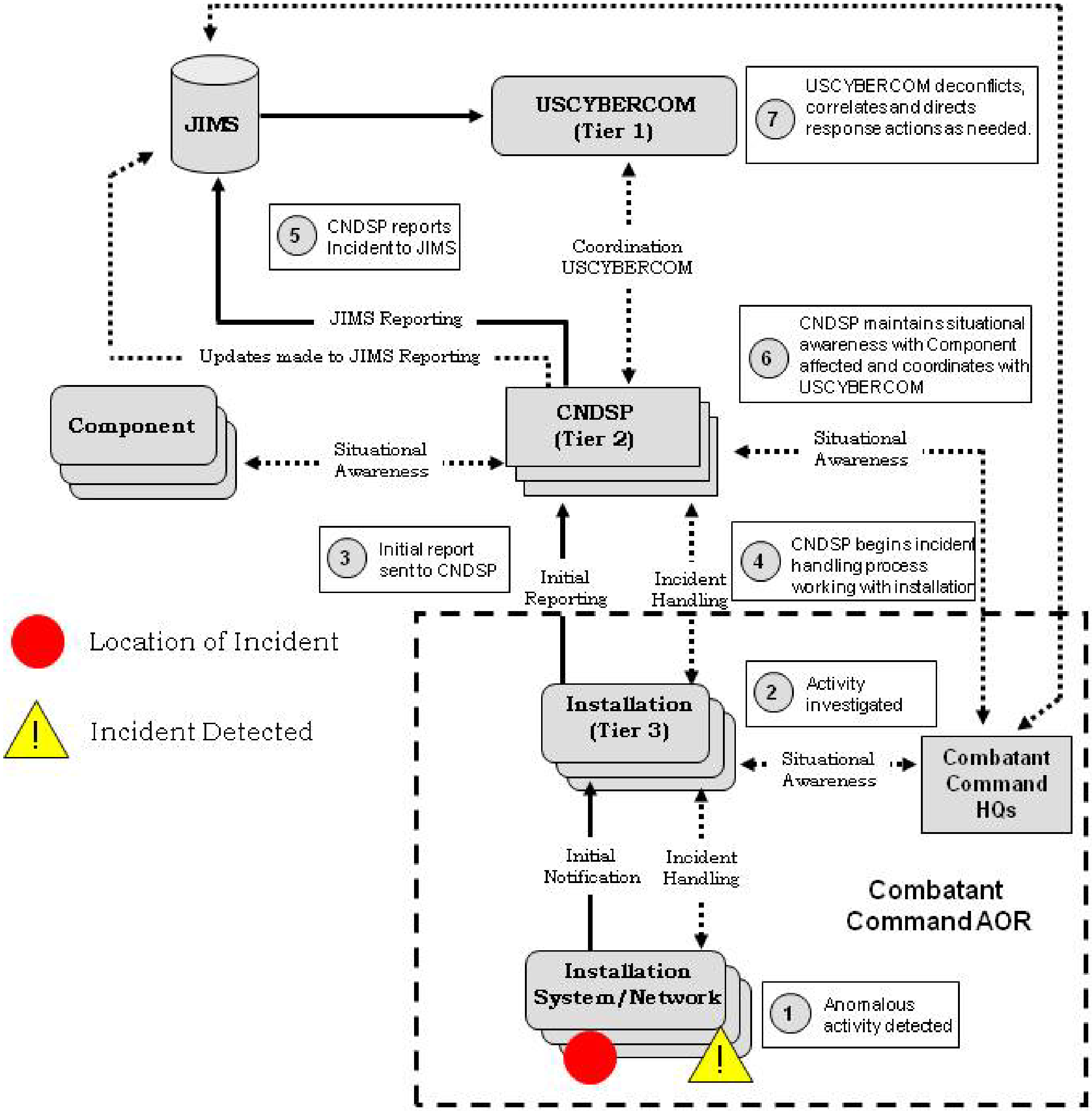

JIMS
USCYBERCOM (Tier 1)
7 USCYBERCOM deconflicts, correlates and directs response actions as needed.
5 CNDSP reports Incident to JIMS
Coordination USCYBERCOM
JIMS Reporting
Updates made to JIMS Reporting
6 CNDSP maintains situational awareness with Component affected and coordinates with USCYBERCOM
Component
Situational Awareness
CNDSP (Tier 2)
Situational Awareness
3 Initial report sent to CNDSP
Initial Reporting
Incident Handling
4 CNDSP begins incident handling process working with installation
Location of Incident
Incident Detected
Installation (Tier 3)
2 Activity investigated
Situational Awareness
Combatant Command HQs
Initial Notification
Incident Handling
Combatant Command AOR
Installation System/Network
1 Anomalous activity detected

Figure C-C-3. Cyber Event Detected Within Combatant Command

4. Cyber Event Detected by External CND Group. The following reporting scenario depicts the general process for reporting incidents detected by an external entity affecting a DoD installation (e.g., B/P/C/S).

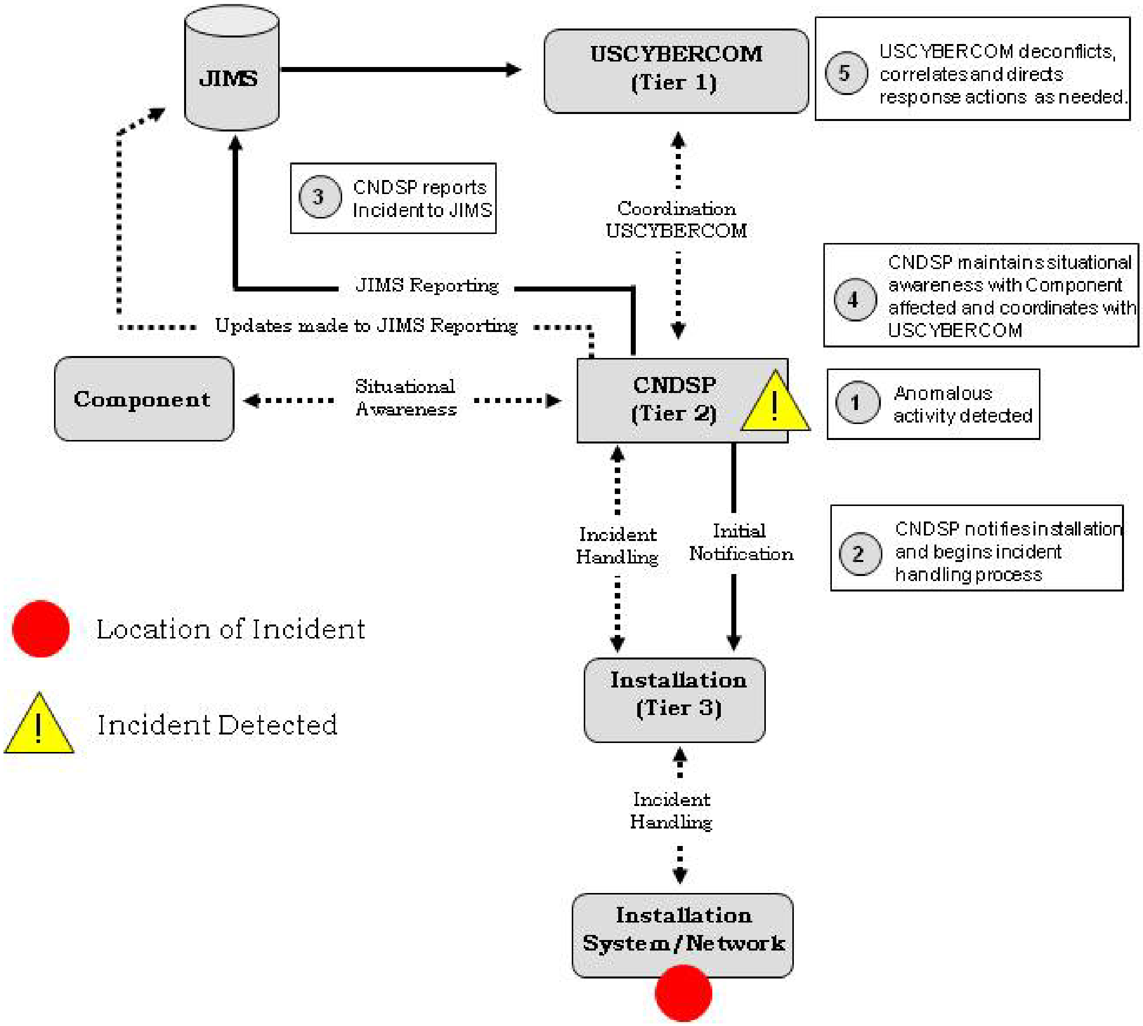

JIMS
USCYBERCOM (Tier 1)
5 USCYBERCOM deconflicts, correlates and directs response actions as needed.
3 CNDSP reports Incident to JIMS
Coordination USCYBERCOM
JIMS Reporting
4 CNDSP maintains situational awareness with Component affected and coordinates with USCYBERCOM
Updates made to JIMS Reporting
Component
Situational Awareness
CNDSP (Tier 2)
1 Anomalous activity detected
Incident Handling
Initial Notification
2 CNDSP notifies installation and begins incident handling process
Location of Incident
Incident Detected
Installation (Tier 3)
Incident Handling
Installation System/Network

Figure C-C-4. Cyber Event Detected by External CND Group

5. Cyber Event Detected by Computer Network Defense Service Provider. The following reporting scenario depicts the general process for reporting incidents detected by a Tier II CNDSP affecting a DoD installation (e.g., B/P/C/S).

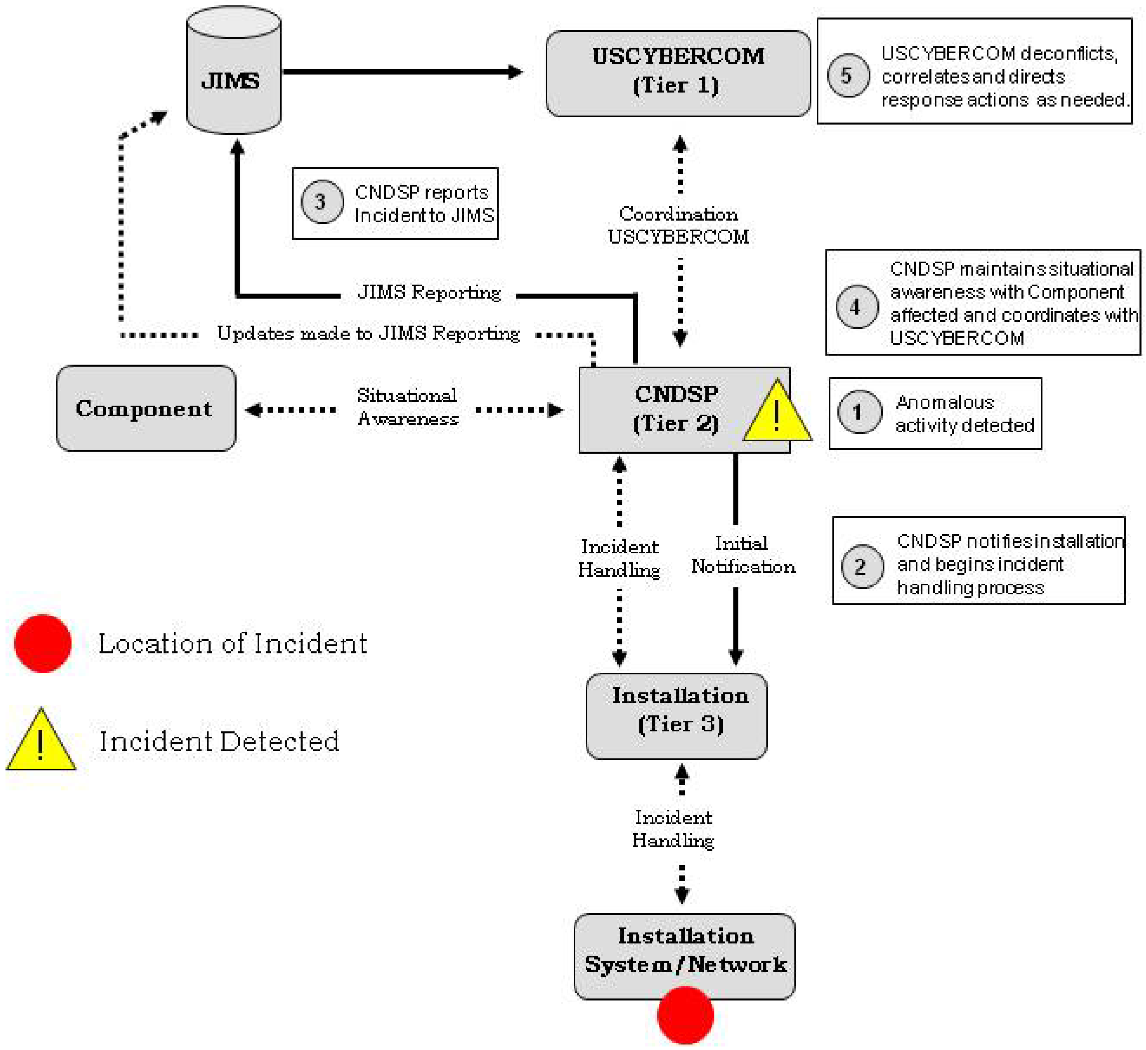

JIMS
USCYBERCOM (Tier 1)
5 USCYBERCOM deconflicts, correlates and directs response actions as needed.
3 CNDSP reports Incident to JIMS
Coordination USCYBERCOM
JIMS Reporting
Updates made to JIMS Reporting
4 CNDSP maintains situational awareness with Component affected and coordinates with USCYBERCOM
Component
Situational Awareness
CNDSP (Tier 2)
1 Anomalous activity detected
Incident Handling
Initial Notification
2 CNDSP notifies installation and begins incident handling process
● Location of Incident
⚠ Incident Detected
Installation (Tier 3)
Incident Handling
Installation System/Network

Figure C-C-5. Cyber Event Detected by CNDSP

(INTENTIONALLY BLANK)

ENCLOSURE D

CYBER INCIDENT ANALYSIS

1. Introduction

a. Incident analysis is the series of analytical steps taken to determine what occurred 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 to establish what additional information to gather, how to coordinate information sharing with others, and how to develop a COA and response. If there is a chance the incident might require the pursuit of disciplinary or criminal actions, the appropriate LE/CI organization must be contacted to ensure proper legal procedures are taken in the investigation of the incident.

b. This section provides additional guidance on incident analysis requirements for reportable events and incidents. Further requirements will be articulated in OPORDs issued by relevant commands.

c. The primary objectives for the incident analysis process are:

(1) Identify the root cause(s) of the incident through technical analysis.

(2) Ensure the accuracy and completeness of incident reports.

(3) Characterize and communicate the potential impact of the incident.

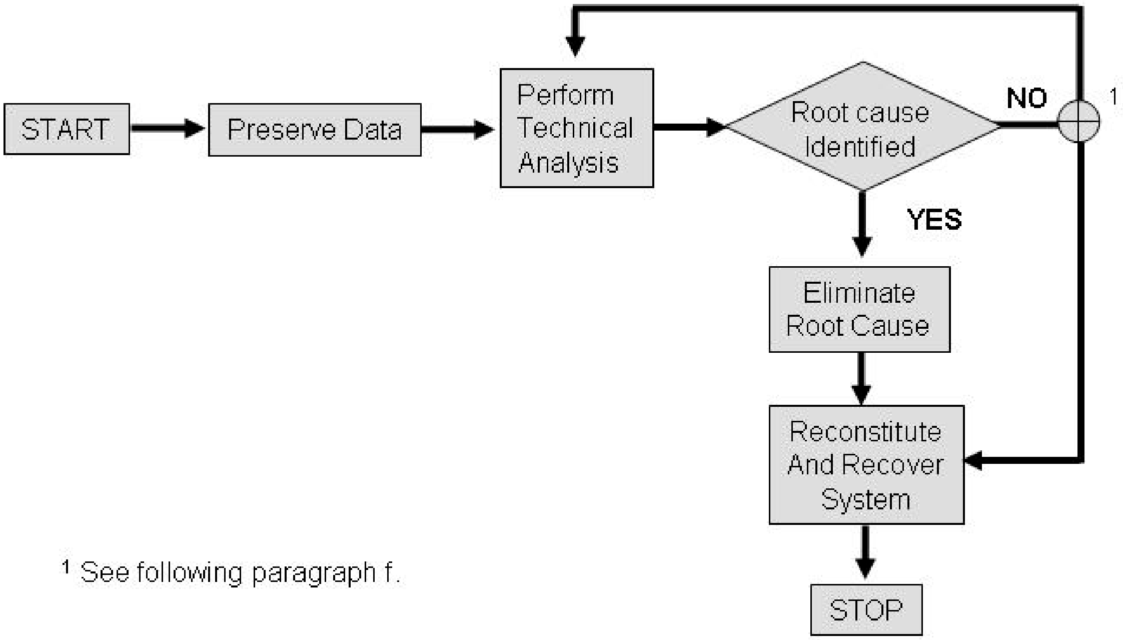
(4) Capture the methods used in the attack and the security controls that could prevent future occurrences.

(5) Research actions that can be taken to respond to and eradicate the risk and/or threat.

(6) Understand patterns of activity to characterize the threat and direct protective and defensive strategies,

d. Technical analysis is iterative in nature. It is conducted many times throughout the incident handling life cycle. Some degree of analysis must occur in order to detect and adequately report an incident. Once an incident has been reported, it may go through several levels of analysis to identify the root cause(s). Each successive level requires personnel that possess more sophisticated skills and have access to additional tools or systems.

e. Incident analysis seeks to identify the root cause(s) of an incident and is required to fully understand the scope, potential implications, and extent of damage resulting from the incident. Figure D-1 below illustrates the basic relationship between data preservation, technical analysis, root cause identification, and IS recovery. Depending on the complexity of the incident and the level of analysis required, the amount of time necessary to analyze an incident may vary from minutes to hours to months.



[1] See following paragraph f.

Figure D-1. Cyber Incident Analysis Relationship to Preserving Data and Recovering Systems

f. In some cases, technical analysis may not be able to conclusively identify the root cause of an incident. The intruder may have deleted or tampered with logs and files, making them untrustworthy, or the existence of multiple unpatched vulnerabilities may make it impossible (or not worth the effort) to try to identify which specific vulnerability was exploited. In such cases, it may be more expedient simply to begin IS recovery and hardening.

g. The decision to restore an IS without identifying the root cause(s) of the incident must be weighed carefully as it may leave the IS vulnerable. For example, if the root cause of an incident stemmed from a missing patch in the baseline configuration, an IS restoration using the same baseline configuration will leave the IS open to future compromise.

2. Cyber Incident Analysis Framework

a. The type of analysis conducted will depend on the nature of the incident under analysis. Typically, responding to an incident will require some combination of the following types of analysis:

(1) System Analysis. The process of acquiring, preserving, and analyzing IS artifacts (e.g., log files or registry information, creating an image, or capturing a screen shot) that help characterize the incident and develop COA.

(2) Malware Analysis. The process of identifying, analyzing, and characterizing reported software artifacts suspected of being adversarial tradecraft to help defense in depth mitigation actions and strategies, CI activities, and LE activities.

(3) Network Analysis. The process of collecting, examining, and interpreting network traffic to identify and respond to events that violate the security policy or posture of the resources attached to the information network or the network infrastructure and used to support computer security incident investigations. Network incident analysis will include the networks log file to show the threat (e.g., router logs, firewall logs, IDS/IPS logs).

b. This set of categories is somewhat arbitrary, as there are no clear lines of separation between them. For example, malware may leave traces on an IS under analysis, as well as in network data. The principles of sound forensic data collection and analysis, particularly in cases that may lead to legal prosecutions, apply across all the above types of analysis.

c. The level, or depth, of analysis conducted can often depend on the context of the analysis request or mission of the organization. For instance, some organizations may be tasked with recovering from a compromise and wish to determine the extent of the damage. This may differ greatly from analysis required to support a law enforcement investigation where data preservation and chain of custody must be strictly managed.

d. The level of incident analysis to be conducted will also vary depending on the incident category, the operational and technical impacts, and any identifiable delivery vectors or IS weaknesses. It will also depend on the availability of relevant information for analysis and available resources.

3. Computer Forensics Analysis

a. Computer forensics is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody. Guidance on integrating forensic techniques into incident response can be found in NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response" (reference o).

b. CNDSPs will establish and maintain a computer forensics program IAW the Evaluators Scoring Metrics for the Certification and Accreditation of CNDSPs. A computer forensics program will include the following:

(1) Policies, including criteria for determining when forensics collection and analysis should be performed.

(2) Guidelines and procedures for forensic collection of evidence, forensics analysis, and chain of custody.

(3) Forensics staff, technology, and facility resources—including trained and knowledgeable staff, tools, and equipment for forensics collection and analysis of evidence—and necessary infrastructure, such as a forensics lab.

c. Many forensics collection and analysis tasks are similar to or overlap with other incident analysis activities, which are generally more focused on gaining a technical understanding of the incident. When these information-gathering and analysis activities are performed for forensics purposes, the forensic activities focus on processing and preserving the authenticity and integrity of the data in a manner that ensures the evidence can be admissible in a court of law.

d. For incidents to be investigated for computer crime, incident handlers and first responders must understand proper forensics and evidence handling policies and procedures, even if that means keeping "hands off" until a trained analyst can start the proper evidence collection. Data and information to be gathered for forensics analysis or evidence must be obtained and handled IAW various applicable laws, possibly spanning many jurisdictions, in order to ensure the authenticity and reliability of the information for forensics analysis as well as to be admissible in a court.

e. Electronic data from a computer to be used for forensics and/or evidence can consist of both volatile data and persistent data from the affected IS(s) (see paragraph 4 (System Analysis)). The use of approved forensics tools and methods to collect and handle volatile and non-volatile data will help ensure that incident handlers and first responders satisfy forensics and evidence requirements.

f. Forensics Process

(1) One model for the forensics process, presented in NIST 800-86 (reference o), describes four basic phases:

(a) Collection. The first phase in the process is to identify, label, record, and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data. Collection is typically performed in a timely manner because of the likelihood of losing dynamic data such as current network connections as well as data from battery-powered devices (e.g., cell phones or Personal Digital Assistants).

(b) Examination. Examinations involve forensically processing large amounts of collected data. A combination of automated and manual methods is used to assess and extract data of particular interest while preserving its integrity.

(c) Analysis. The next phase is to analyze the results of the examination, using legally justifiable methods and techniques, to derive information that addresses the questions driving the analysis.

(d) Reporting. The final phase is reporting the results of the analysis. This may include describing the methods used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. The formality of the reporting step varies greatly depending on the situation.

(2) The reporting phase of forensics can also present the evidence and the results of the analysis in a court of law. Individuals involved in conducting any activities for forensics purposes (particularly the collection phase) must understand the forensics process and be prepared to explain their actions in court.

g. Forensics Policies, Guidelines, and Procedures

(1) In accordance with NIST 800-86 (reference o), forensics policies “should allow authorized personnel to monitor systems and networks and perform investigations for legitimate reasons under appropriate circumstances.” In addition, each organization “should ensure that their policies contain clear statements that address all major forensic considerations, such as contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies, guidelines, and

procedures." CC/S/A/FAs, CND incident handlers, and first responders must understand and abide by their organization's forensics policies.

(2) Forensics Guidelines and Procedures

(a) NIST 800-86 (reference o) provides organizations a starting point for developing a forensic capability, in conjunction with extensive guidance provided by legal advisors, law enforcement officials, and management.

(b) The guidelines and procedures should support the admissibility of evidence into legal proceedings including:

1. Information on gathering and handling evidence properly.

2. Preserving the integrity of tools and equipment.

3. Maintaining the chain of custody.

4. Storing evidence securely.

(c) Although it may not be feasible to record every event or action taken in response to an incident, having a record of the major events and actions taken help to ensure that nothing has been overlooked and explains how the incident was handled. This documentation can be useful for case management, report writing, and testifying. Keeping a record of the dates and times that people worked on an incident, including the time needed to recover ISs, can also help calculate the costs of damages. Also, handling evidence in a forensically sound manner puts decision makers in a position where they can confidently take the necessary actions.

(d) Guidelines and procedures for forensics evidence collection, handling, and analysis will be more extensive and less flexible than those for general incident data collection and analysis. Forensics processing requirements generally exceed typical incident collection and analysis procedures in the following areas:

1. Increased preparation and use of specialized tools for acquisition and analysis of evidence.

2. Increased level of detail in documenting the scene (e.g., recording model numbers and serial numbers of equipment, photographing hardware, peripherals, wiring and network connections, photographing the monitor/screen, etc.).

3. Stricter attention to the order in which volatile system data is acquired (to avoid loss of volatile data).

4. Increased care taken to capture persistent data while preventing contamination of evidence (e.g., removing/seizing hard drives and storage media, or creating forensically sound duplicate images on prepared storage devices; using hardware and/or software write blockers to prevent changes to data; and creating hashes of the suspect data and duplicate images to verify authenticity).

5. Increased documentation of steps taken during evidence examination and analysis (including date- and time-stamping of all actions taken).

6. Increased controls limiting access to evidence and maintenance of a chain of custody.

7. Different details to be included in reports of the analysis results (different audience).

8. Different evidence storage/retention timeframes, policies, and procedures.

4. System Analysis

a. System analysis is the gathering and review of all information from or about the affected IS(s) to further incident analysis and understand the full scope of the incident. The IS information to be analyzed typically includes various logs, files, configuration settings, records of currently logged-on users, past connections (logins), running processes, open files, and changes to files or system settings (access control lists (ACLs), registries, and permissions).

b. If the IS has been compromised, care must be taken when using any programs on the suspect IS that may have been modified, or in trusting the validity of logs that may have been tampered with and altered, replaced, or removed. A CND or incident response toolkit, containing trusted copies of system analysis tools, should be used. The toolkit should include appropriate OS tools to examine the suspect IS, including tools to analyze:

(1) Files and logs—examine text files, binary/executable files, and archive files.

(2) Processes—list processes and list processes that open a socket.

(3) Connections—list open sockets or ports; list ISs that recently connected.

c. As part of the data collection effort, the first responder must determine what has been done to an IS and by whom. This includes not just the attacker, but system and network administrators and IS users. The first responder should have an initial set of questions to ask to those involved and a log book for recording all the information gathered. First responders must document everything they can, including all actions they or anyone else involved take during the investigation or response. A new log must be created for every incident or case. During data collection, the first responder will document the following in the log book:

(1) Who is performing the forensic collection.

(2) The history of executed analytical tools and commands done during the collection.

(3) Any generated tool and command output.

(4) The date and time of the executed commands and tools.

(5) Expected IS changes or effects (e.g., changed media access control times for specific files) as first responder tools are executed.

(6) Any other information pertaining to the response, including artifacts or notes about the IS, its configuration, and its physical location.

d. Data obtained for forensics analysis or evidence must be collected using forensically sound methods and tools that capture the relevant data while preventing or minimizing evidence contamination. Forensics methods and tools are specifically designed to enable the following:

(1) **Collection of volatile data** while minimizing the footprint left on the suspect IS. Volatile data is any data stored in IS memory (system registers, cache, and RAM) that will be lost when the IS loses power or is shut down. If the IS is rebooted or shut down, this data may be permanently lost. Examination of volatile data can provide insight into the state of the IS and currently running processes, and potentially help determine a logical timeline identifying the date, time, and/or cause of the incident.

(2) **Collection of persistent data** while preventing data on the suspect IS from being overwritten. Persistent data includes data in the IS's hard drives and removable storage media that will not be changed when the IS is powered off. This often includes disk imaging, the process of creating an exact

duplication of the original disk. A disk image includes files as well as hidden files, deleted data, slack space, swap files, and unallocated space.

(3) **Documentation of the process,** typically using a forensic collection log book. The documentation should contain a time-stamped record of all actions taken during collection of the evidence. The purpose of the documentation is to enable the process to be validated and ensure that the digital evidence is an exact representation of the original data.

e. Detailed steps for conducting system analysis on various OSs and equipment are beyond the scope of this manual. The analyst who performs such analyses, however, must be knowledgeable and have the necessary tools to access and examine the following types of information on the affected IS(s):

(1) Volatile Data. Any data stored in IS memory (system registers, cache, and RAM) that will be lost when the IS loses power or is shut down.

(a) Volatile IS data and time examples include:

1. IS profile.

2. Current IS data and time.

3. Command history.

4. Current IS uptime.

5. Running processes.

6. Open files, startup files, and clipboard data.

7. Logged on users.

8. Dynamic-linked libraries (DLLs) or shared libraries.

(b) Volatile network data examples include:

1. Open connections.

2. Open ports and sockets.

3. Routing information and configuration.

4. Network interface status and configuration.

5. Address resolution protocol (ARP) cache.

(2) Persistent (Non-Volatile) Data. Data in the IS's hard drives and removable storage media that will not be changed when the IS is powered off. Examples include the following:

1. IS log files.

2. Event Viewer files.

3. Application logs.

4. Disk image—exact duplicate of the original disk, which includes files as well as hidden files, deleted data, slack space, swap files, and unallocated space.

f. While conducting the system analysis, the analyst may need to perform other related tasks. These tasks include looking up hostnames and IP addresses or tracing them back to their sources; searching for hidden or deleted files; checking the integrity of system binaries; checking for unauthorized processes or services; identifying potential malware; or examining other machines on the local network.

g. After the system analysis has been completed, new details will emerge, requiring a follow-on report. Information fields in the initial incident report may also need to be updated.

h. For a summary of resources useful for investigating incidents, refer to the DOJ "Investigations Involving the Internet and Computer Networks" (reference p).

5. Malware Analysis

a. Malware analysis is the process of analyzing and capturing the capabilities of software artifacts suspected of being malicious code. It is an essential step in determining the full scope of an incident. Malware is defined as software designed and/or deployed by adversaries without the consent or knowledge of the user in support of adversarial missions (e.g., gaining access to resources or information, cyber strikes, C2 operations).

b. Uncovering an adversary's tools, techniques, procedures, and motivations will aid in discovering other affected or vulnerable ISs, establishing a more concrete framework for attribution, and development of additional defensive measures.

c. Individuals analyzing or otherwise handling malware are expected to:

(1) Handle with Care. Adversarial tradecraft is employed by the adversary as a weapon and should be handled as such. It is important when handling a sample suspected of being malicious that proper care is taken to ensure that the sample does not affect any operational DoD information networks or ISs. If possible, once a sample is identified, it should be moved to a separate IS that is completely isolated for analysis. Any physical media used to transport samples should be labeled to indicate that its contents are potentially malicious.

(2) Catalog all Software Artifacts. All artifacts suspected of being malware should be safely acquired, preserved, and submitted to the authorized malware catalogs for storage.

(3) Manage Capability Effectively. Due to the large volume of artifacts that will likely be gathered as part of system analysis, and because the process of analyzing malware can be extremely time and resource intensive, it is unlikely that a complete, end-to-end analysis of every artifact identified as malicious will be feasible. For this reason, it is important for all DoD CND personnel to understand the analytical resources available to them and to apply a measure of cost-benefit analysis to determine the depth of analysis to be performed on a given artifact. Automated tools should be employed to increase the number of samples that can be processed, where applicable.

(4) Perform Analysis in an Isolated Environment. Precautions must be taken when performing analysis to prevent against the execution of code that may adversely affect DoD information networks or ISs. Malware analysis shall be done in a safe and isolated environment segregated from other ISs. In this isolated environment, the intentional or unintentional, execution of the code does not violate the implicit or explicit security policies of the IS. For example, isolated environments may include a malware analysis laboratory, virtualization environment, or an analyst workstation disconnected from the network and intended for malware analysis. This prevents the unintentional compromise of additional ISs or sensitive information.

d. Establish Policies Governing Media That Can be Connected to an Analysis Machine. For example, it is relatively common for malware to use universal serial bus (USB) keys to spread, so policy governing the usage of USB keys and other forms of portable storage must be established.

e. Preserve the original software artifacts. It is fairly common for malware to attempt to avoid detection by modifying and/or deleting the original malicious file(s). The malware file(s) should be transferred between ISs by a means that avoids accidental execution and preserves evidentiary admissibility.

Where feasible, technical solutions that physically or electronically prohibit malware distribution should be implemented.

f. Levels of Depth for Malware Analysis

(1) Malware analysis can be performed at varying degrees of depth. Each successive level requires personnel who possess more sophisticated skills and have access to additional tools or ISs. Depending on the complexity of the malware and depth of analysis required, the time necessary to complete the request can vary from minutes to hours to months. Therefore, when requesting malware analysis, asking specific questions about information of interest to the mission helps expedite results.

(2) The diagram (Figure D-2) below illustrates the different degrees of depth for malware analysis. After each stage, the decision must be made as to whether additional information is needed. If additional information is needed, the next successive level of analysis begins. If no additional data is needed, then the analysis should be recorded and appropriately communicated.

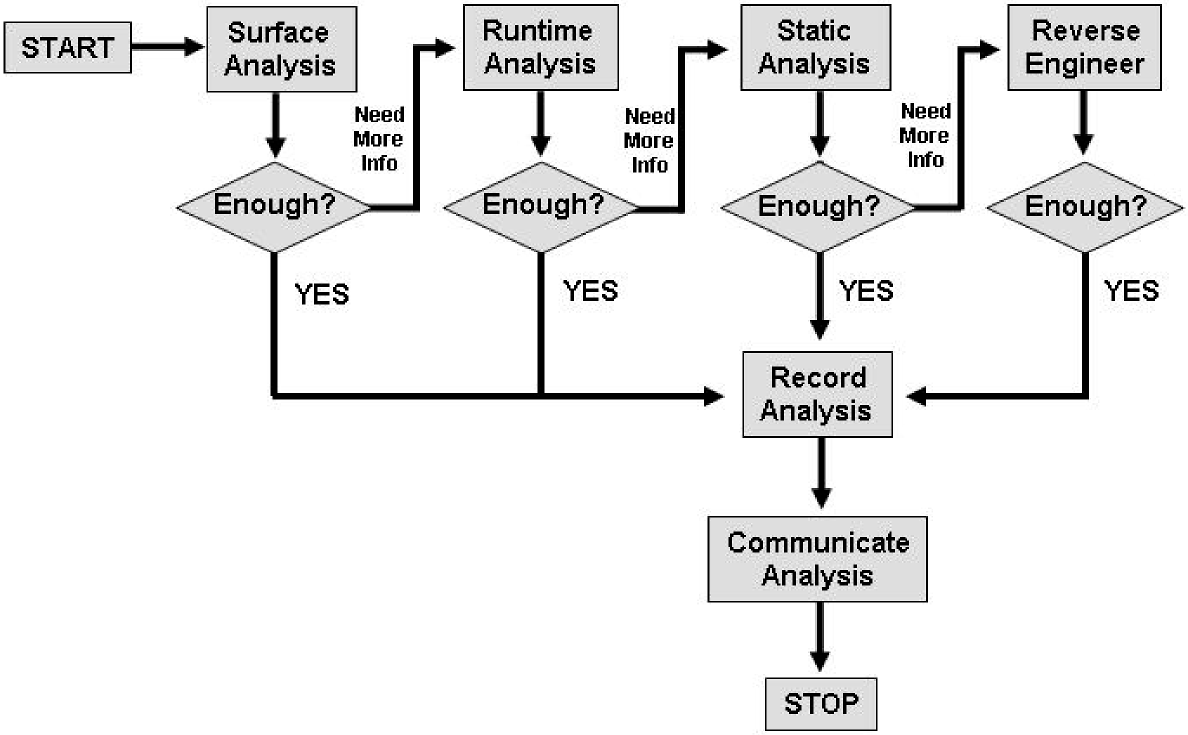


Figure D-2. Levels of Depth for Malware Analysis

(3) Surface Analysis

(a) Surface analysis involves quick checks to characterize the sample within the context of the analysis mission.

(b) Common surface analysis techniques include file type identification, strings extraction, public source analysis, and comparative analysis with previously analyzed artifacts. The results of this analysis should either produce an actionable result in the context of the request or be used to help direct additional analysis as required

(c) Potential information to be gained through surface analysis includes the following:

1. Basic determination of nature and intent.

2. Identification of strings in binary files.

3. Cryptographic hashes.

4. Antivirus software detection status.

5. File sizes.

6. File type identification.

7. File attribute information.

8. Packer identification.

9. Signature-based detection status.

(d) While useful for quick malware characterization, surface analysis can produce results based on an incomplete picture of the malware sample. Surface analysis does not accurately determine program functionality. For example, surface analysis may produce useful matches against third-party information, but the third-party information may be incomplete or inaccurate.

(e) Analysis missions requiring a high degree of assurance shall not rely solely on surface analysis.

(4) Run-time Analysis

(a) Run-time analysis is the controlled execution of the malware sample in an isolated environment instrumented to monitor, observe, and record run-time behavior without impacting mission-critical systems and infrastructure.

(b) Although run-time analysis may provide additional information relative to surface analysis, run-time analysis is generally limited to observation of default execution paths of malware samples. Malware samples may contain unexercised functionality or demonstrate alternate behavior in different run-time environments.

(c) Potential information to be gained by performing run-time analysis includes:

1. Network touch points (addresses, protocols, ports, etc.).

2. File system and registry activity.

3. Vulnerabilities or weaknesses in particular run-time environments.

4. System service daemon interactions.

5. Dynamic unpacking of packed executable files.

6. Success of remediation techniques in particular run-time environments.

7. Suggestions of adversarial intent (low degree of confidence).

(d) Note: Subsequent surface analysis of unpacked binaries may yield additional results, and could possibly negate the need for further resource expenditure.

(5) Static Analysis

(a) Static analysis focuses on examining and interpreting the contents of the malware sample in the context of an analysis mission. Files of many types, particularly text files, Web page scripts, and source code files can be analyzed without malware sample execution or disassembly. In the case of a binary, if a complete understanding of the malware sample is necessary, reverse engineering is required.

(b) Potential information to be gained by performing static analysis includes:

1. Static unpacking of packed executables.

2. Definitive understanding of program source code.

3. Determination of adversarial intent (high degree of confidence).

4. Deobfuscation of obfuscated data.

(6) Reverse Engineering

(a) Reverse engineering, the most in-depth analysis, is highly complex and consists of disassembly of malware sample executable files and interpretation of the assembly language. Reverse engineering is time-intensive and requires extensive technical knowledge and specialized tools. It is the only method of analysis that can produce a definitive or complete understanding of a malware sample. Reverse engineering analysis can range from addressing particular problem scope in order to answer a very few specific questions to extensive reverse engineering all of the code in a malware sample in order to understand complete functionality.

(b) Potential information to be gained by performing reverse engineering includes:

1. Manual unpacking of packed executable files.

2. Understanding of obfuscation or encryption techniques.

3. Definitive understanding of malware capabilities.

4. Characterization of malware sophistication.

5. Comparison of capabilities across malware samples.

g. Cataloging Malicious Code

(1) All software artifacts suspected of being malware must be safely acquired, preserved, and cataloged.

(2) Cataloging of incident-related artifacts provides structured storage of pertinent malware, logs, and related analysis. Any malware uncovered throughout the incident response process must be cataloged to the JMC. Additional guidance may be found in Enclosure G (Cyber Incident Handling Tools—Joint Malware Catalog). Maintaining a central catalog facilitates and enhances correlation and information sharing within the DoD incident response community.

(3) Any analytical products that are created should be shared safely, both horizontally and vertically, to the greatest extent possible to ensure that the resources expended can be best utilized to improve the Department of Defense's overall situational awareness and defensive posture.

h. Requesting Malware Analysis

(1) Analysis of malware samples is required to accurately characterize the capabilities of the malware. The scope, complexity, and depth of malware analysis requests may differ across DoD and CND organizations. For instance, some components may be tasked with recovering from a compromise and wish to determine the extent of damage done. Intelligence organizations may conduct analysis to gain technical insights to support attribution, or to support counterintelligence activities.

(2) When requesting malware analysis, the requestor should specify the questions about the malware requiring an answer and identify any specific information required to support the mission. Malware analysis is resource intensive, and the depth of analysis performed should be no more than is absolutely required. Effective management of analysis requests is critical to managing an effective malware analysis capability.

(3) When requesting analysis of a malware sample, Table D-1 should be used to assist in specifying the analysis information required within the context of the mission.

Level of Analysis	Information Produced from Analysis
Surface Analysis Determine basic nature and intent	− Identification of strings in binary files − Cryptographic hashes − Antivirus software detection status − File sizes − File type identification − File attribute information − Packer identification − Signature-based detection status
Runtime Analysis Determine adversarial intent with low degree of confidence	− Network touch points (addresses, protocols, ports, etc.) − File system and registry activity − Vulnerabilities or weaknesses in particular run-time environments − System service daemon interactions − Dynamic unpacking of packed executable files − Success of remediation techniques in particular run-time environments
Static Analysis	− Static unpacking of packed executables

Determine adversarial intent with high degree of confidence	− Definitive understanding of some portion of program source − Deobfuscation of obfuscated data
Reverse Engineering Definitive understanding of malware analysis capabilities	− Manual unpacking of packed executable files − Understanding of obfuscation or encryption techniques − Definitive understanding of malware capabilities − Characterization of malware sophistication − Comparison of capabilities across malware samples

Table D-1. Levels of Analysis for Requesting Malware Analysis

6. Network Analysis

a. Network security analysis consists of the collection, examination, and interpretation of network traffic to identify and respond to events that violate the security policy or posture of the resources attached to the network or the network infrastructure.

b. Analyzing an adversary's use of network resources, and uncovering the network interactions that occurred during an intrusion, aid in discovering other affected or vulnerable ISs. It also helps in the development of additional defensive measures.

c. Network analysis should be an ongoing activity, with analysts constantly studying and monitoring the normal operation of the network. This should include constructing and updating a baseline of the inventory of hosts and application servers. Because the most serious incidents may not be detected by automated analysis or IDS, analyst understanding of the network provides the best chance of noticing unusual patterns associated with the malicious activity. Once in an incident response situation, this preparatory work will pay significant dividends as the incident response team works through the process described in Enclosure B (Cyber Incident Handling Methodology).

d. Network Analysis Capabilities. The network analysis capabilities required for CND analysis across the Department of Defense include the following:

(1) I&W. Appropriate use of intelligence information to understand the threats to the DoD information network (both external and internal).

(2) AS&W. Detection of known and suspected malicious activity, as well as sharing of such information for improved I&W capability across the Department of Defense.

(3) Situational Awareness. Situational awareness is understanding the current network security posture, including internal assets and their vulnerabilities, normal and abnormal traffic patterns, and defensive measures in place. These goals are interdependent and none can be fully achieved without the others.

e. Network Analysis Technologies

(1) Some fundamental technology approaches that form the building blocks of network analysis capabilities include:

(a) Wire speed network capture and/or examination.

(b) Traffic summarization.

(c) Pattern matching.

(d) Protocol analysis at all layers of the protocol stack.

(e) Behavioral analysis.

(f) Statistical anomaly detection.

(g) Correlation between data sources.

(2) All network monitoring technologies should be provisioned, configured, and evaluated to achieve the following minimum requirements:

(a) The ability to operate at the bandwidth levels experienced at the deployment point, up to and including link saturation, while successfully collecting and/or examining all traffic (no packet loss or loss of capability).

(b) Pattern matching engines support "regular expressions" or a similarly flexible pattern expression language.

(c) Signature engines permit the operator to provide custom signatures, to permit DoD-specific signature development according to timely I&W information.

(d) Network sensors perform IP fragment reassembly, to ensure correct parsing of transport layer headers.

(e) Network sensors that examine the application layer perform Transmission Control Protocol (TCP) stream reassembly to ensure correct parsing of content data. While there is some difficulty in the emulation of the behavior of TCP/IP stacks on destination hosts (e.g., differences in the handling of urgent pointers), a generic reassembly protocol is sufficient to fulfill the requirement.

(f) Anomaly detectors achieve acceptable accuracy rates, as defined by the alert consumers, including appropriate or adjustable parameter settings to maximize accuracy in the deployed information network.

f. Network Analysis Methodology. Network analysis comprises data sources, data collection, and data analysis.

(1) Data Sources. Network traffic consists of event, session, full content, and statistical data.

(a) The availability of data sources will vary based on the complexity of the information network and level of network instrumentation in place.

(b) Acquiring some data sources may require coordination across DoD elements. This data may reside on the local workstations, network devices, monitoring instrumentation, or other network security mechanisms.

(2) Data Collection. The collection of data focuses on gathering network and transport header information (particularly source and destination addresses and ports), content and content-based information (from full packet capture to specific application parameters such as Uniform Resource Locators (URLs) or domain resolution data), traffic summaries, and alerts based on matches on patterns or models of malicious activity (e.g., IDS alerts). Specific technologies that provide this information change over time to address new threats and to incorporate novel approaches to address new and existing threats. However, all DoD entities (or their CNDSPs) must, at a minimum, collect data from the following sources:

(a) Network Log Data. This data includes logs of all network connections passing the network boundary at a connection summary level (e.g., network flow records or firewall logs) or better, with a log retention policy that prioritizes data retention. Collecting network logs internally (internal routers or switches) would further enhance this capability. The entity, or its CND service provider, must have an active program of monitoring and analyzing its network log data.

(b) Intrusion Detection Data. This must include at least pattern matching capability, with an active signature management program to responsibly address current threat information as available to the incident response organization. In general, vendor-provided signatures would need to be supplemented with DoD-specific signatures to address targeted threats, according to currently available I&W information.

(3) Enhanced capabilities can be achieved by additionally collecting the following types of data:

(a) Full Packet Capture Data. This data can provide complete insight into network transactions that occurred between hosts. It can also allow for the reconstruction of network sessions that can provide a better characterization of the activity. Full packet capturing enhances network logging capability, but must be balanced with the increased cost and analytical overhead due to the much larger data volumes involved. Data retention would typically be much shorter than for summary log data.

(b) Statistical and Behavioral Anomaly Detection Data and/or Protocol Analysis. This data can enhance IDS capabilities and contribute to a deeper understanding of network behavior. However, the benefits must be balanced with the uncertainty inherent in these approaches.

(c) Intrusion Prevention System Data. This data can be used to identify known malicious activity or attempted intrusions. IPSs may enhance network protection by blocking known malicious traffic, but their benefits must be balanced with the potential for interference with production traffic. These systems must be tuned to minimize false positives; this means that intrusion detection capabilities (which may simply mean non-blocking signatures on the same device) must still be provided to detect intrusions missed by the tighter configuration of the IPS.

(4) Data Analysis. Network data analysis helps identify anomalous and potentially malicious activity, enumerate network resources involved in an intrusion, and identify other ISs that may be affected. System and malware analysis will generally also be required to piece together the full event timeline. Many exploits may not be identifiable as such based solely on network activity, for example. Some types of analysis that may be required include the following:

(a) Timeline Reconstruction. What did the attacker do? Identify the relevant hosts, network connections, and application events, and place these into an event timeline to organize the information about the incident. This timeline would be used to correlate other event information gained from analysis of system logs, file timestamps, etc.

(b) Exploit Analysis. What was exploited and how? Examine all the traffic data sources in order to determine the nature of the exploit and assist in identifying the root cause(s) of the incident. The analyst will have to understand the protocols involved and the network manifestation of the exploit.

(c) Retrospective Analysis. What else did the attacker do? Use traffic summaries or packet capture data to reconstruct past network events relevant to the intrusion, potentially identifying portions of the malicious activity that were missed by IDS systems. This analysis is part of the process of identifying the full scope of the intrusion event. The analyst will often have to iterate through the other types of analysis, adding new events to the timeline and determining root cause(s) of other exploit activity.

g. Analysts must have strong command of the analysis tools at their disposal, and their organizations should support providing the analyst with the specialized training and continuing education to perform well in their role. An automated analysis or alerting tool can only provide the beginning of an understanding of a security incident, and only a skilled analyst provided with appropriate tools can complete the picture.

7. Analysis and Correlation of Event and Incident Data. Analysis and correlation of event and incident data occur at all levels, as well as within various functional communities (e.g., intelligence, counterintelligence, LE). To conduct this analysis and correlation, it is important that all tiers participate in comprehensive support of the reporting process. Correlation of data enables the CC/S/A/FAs to identify traffic patterns, trends, and other relevant information that is used in determining the defensive operational picture.

8. Legal Issues. The following is provided as background information on legal issues impacting on incident analysis.

a. A number of federal laws[7] affect the monitoring and collection of electronic communications and data. These laws cover various topics, such as the searching and seizing of computers and data, privacy, electronic surveillance, and rules of evidence.

(1) Laws governing the monitoring of data in transit can be found in 18 U.S.C. section 2510 et seq. (reference q) and 18 U.S.C. section 31212 et seq. (reference r) and found in 18 U.S.C. section 2701 et seq. for data in storage (reference s).

(2) There may be additional state and local laws (or international laws) that similarly affect forensics activities.

[7] Relevant laws include the U.S. Constitution (4th and 5th amendments), U.S statutory law (18 U.S.C. sections 2510-22, 2701-12, 3121- 27), and Federal Rules of Evidence (hearsay, authentication, and identification). For more information, see http://www.cybercrime.gov/.

b. Incident handlers and first responders will conduct data acquisition for forensics evidence IAW guidance provided by legal advisors, law enforcement officials, and management.

c. For example, computer records are generally admitted as evidence under the Federal Rules of Evidence Exception (803(6)) (reference t) for **records of regularly conducted activity**. If documented policies and procedures regarding network monitoring and incident response are followed, this will help computer records to be admitted under this Federal Rules of Evidence Exception (reference t), whereas the lack of policies and procedures (or ad hoc procedures) may not.

d. The DOJ manual "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"[8] (reference u) provides guidance on related topics, including searching and seizing computers with or without a warrant; issues related to the Electronic Communications Privacy Act (ECPA) (reference v); issues related to the electronic surveillance in communications networks (Pen/Trap Statue; Wiretap Statute); and evidence. Although the manual was published to provide guidance to federal law enforcement agents and prosecutors, understanding this guidance will help individuals conducting forensics activities better understand the relevant legal issues that arise and better prepare to interact with law enforcement and prosecutors when needed.

e. The DOJ National Institute of Justice provides additional guidance on digital evidence issues in a series of special reports:

(1) <u>Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition</u>. This report (reference w) includes additional and more detailed guidance on developing policies and procedures, securing and evaluating the scene, handling evidence at the scene, examining the evidence, and documenting and reporting the results. The report also provides lists of potential evidence by crime category.

(2) <u>Forensic Examination of Digital Evidence: A Guide for Law Enforcement</u>. This report (reference x) is intended for law enforcement officers who examine digital evidence. It provides guidance on policy and procedure development; evidence assessment, acquisition, and examination; and documenting and reporting analysis results. Appendices include case examples and sample worksheets.

(3) <u>Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors</u>. This report (reference y) identifies federal laws governing search and seizure issues. It also provides guidance on the handling of digital evidence, courtroom preparation, and presentation of digital evidence.

[8] http://www.justice.gov/criminal/cybercrime/ssmanual/

f. Collection of Evidence. Data obtained for forensics analysis or evidence must be collected using forensically sound methods and tools that capture the relevant data while preventing or minimizing contamination of the evidence.

g. Storage of Evidence

(1) Any data or records that might be used as evidence must be documented, maintained, and protected under a chain of custody in accordance with forensics policies and procedures. This avoids allegations of mishandling or tampering with evidence and increases the probability evidence will be entered into a court proceeding.

(2) A chain-of-custody log is used to document the integrity of any evidence at every point from the time it is seized until it is presented in court. A chain-of-custody log will typically include the following types of information:

(a) Description of the evidence.

(b) Details of where (location), when (date and time), and by whom (name, contact information) the evidence was found.

(c) Detailed description of the forensic evidence collection method, tools, or procedures

(d) Details (who, where, when) of the transfer of evidence to a custodian for safekeeping.

(3) A custodian must be designated to control and keep records of any access to the evidence.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE D

DELIVERY VECTORS

1. Introduction. 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.

2. Delivery Vector Categories

a. 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).

b. This annex 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**
1	**Sub-category**	**Reconnaissance:** Information was accessible and used to characterize ISs, applications, information networks, and users that may be useful in formulating an attack.
	A	Information Gathering and Data Mining: Activity that seeks to gather information from publicly available sources.
	B	Network Scan: Activity that targets multiple IP addresses. This is referred to as a horizontal scan.
	C	System Scan: Activity that targets a single IP address across a range of ports. This is referred to as a vertical scan.

Table D-A-1. Delivery Vectors Categories

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.

Table D-A-1. Delivery Vectors Categories (continued)

Delivery Vector Category Number		**Description**
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 D-A-1. Delivery Vectors Categories (continued)

c. 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.

(INTENTIONALLY BLANK)

APPENDIX B TO ENCLOSURE D

INFORMATION SYSTEM WEAKNESSES

1. Introduction

a. Security controls are safeguards or countermeasures applied to an information system (IS) in order to protect the confidentiality, integrity, and availability of the IS and its information. The catalog of security controls can be found in Committee on National Security Systems Instruction No. 1253, "Security Categorization and Control Selection for National Security Systems" (reference z).

b. Information about IS weaknesses is collected as part of the incident report and used to broadly represent gaps or deficiencies in protective and defensive security controls. Security control effectiveness is defined as the extent to which existing controls are implemented correctly, operating as intended, and producing the desired outcome in meeting the security requirements for the IS in its operational environment.

c. By collecting this information on an ongoing and consistent basis, management can make more informed decisions based on real data and can provide technical direction that significantly improves the protection of DoD information networks.

2. Determining Information System Weaknesses

a. NIST SP 800-60, "Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories" (reference aa), can be used to identify the security family and security control(s) that could have been in place to prevent or lessen the impact of the incident. IS weaknesses must be recorded as part of the incident handling process and included in the incident report. It is expected that more than one security control may apply.

b. For example, an incident that had a missing patch, poor baseline system configuration, and out-of-date AV signatures as its root causes may have the following IS weaknesses associated with it:

(1) Configuration management.

(2) System and information integrity.

c. IS weaknesses are dynamic and may change over time. Applications, processes, and procedures that independently operate and maintain the security controls must be flexible to allow these controls to be modified as needed while minimizing the effects these changes may have on incident reporting activities.

APPENDIX C TO ENCLOSURE D

IMPACT ASSESSMENT MATRIX

1. Impact Assessment

a. 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.

(1) Each cyber event or incident is assessed and assigned an impact as part of the incident handling process.

(2) An impact assessment is one of the determining factors when assigning priority to an incident or event.

(3) The category and impact guide reporting timelines and response actions should be commensurate with the magnitude of the incident or event.

b. In determining the actual impact, consider the current and potential impact of the incident or event on the confidentiality, availability, and integrity of organizational operations, organizational assets, or individuals. The standards and guidelines used below provide a baseline for assessing impact have been adopted and adapted (where necessary) from DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)" (reference bb).

2. Levels of Impact

a. Low. The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(1) Cause degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced.

(2) Result in minor damage to organizational assets.

(3) Result in minor financial loss.

(4) Result in minor harm to individuals.

b. Moderate. The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means, for example, that the loss of confidentiality, integrity, or availability might:

(1) Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.

(2) Result in significant damage to organizational assets.

(3) Result in significant financial loss.

(4) Result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

c. High. The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means, for example, that the loss of confidentiality, integrity, or availability might:

(1) Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions.

(2) Result in major damage to organizational assets.

(3) Result in major financial loss.

(4) Result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

3. Determining Technical and Operational Impact

a. The tables below should be used to identify the potential technical impacts (TIs) and operational impacts (OIs) of the incident or reportable event.

(1) These impacts should be 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.

(2) These impacts must be recorded as part of the incident handling process and included in the incident report.

b. For example, a DoS attack against a local MAC I/II mail server may have the following impacts:

(1) Technical Impact

(a) Confidentiality—Low.

(b) Integrity—Low.

(c) Availability—Medium.

(d) The potential impact to technical availability is medium because it may degrade day-today business services.

(2) Operational Impact

(a) Confidentiality—Low.

(b) Integrity—Low.

(c) Availability—High.

(d) The potential impact to operational availability is high because it is targeted at a MAC I/II IS.

4. Cyber Incident Impact Table. 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	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations,	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or	The unauthorized disclosure of information could be expected to have a **severe** or **catastrophic** adverse effect on organizational operations, organizational

information. [44 U.S.C. 3542].	organizational assets, or individuals.	individuals.	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 U.S.C. 3542].	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 D-C-1. Cyber Incident Impact Table

5. Cyber Incident and Event Potential Impact. The following tables provide examples of incidents or events and how they are categorized across each security objective and impact level.

a. The tables should be used as a guide to determine the potential impact of an incident or event. Initial assessment should be performed quickly even with limited details and analysis.

b. As the investigation continues and a more accurate characterization of the true impact is understood, there is always opportunity to reassess and modify the potential impact.

c. Note: "All Security Objectives" is intended to represent examples of incidents or events that may affect any security objective (i.e., confidentiality, integrity, and availability).

	POTENTIAL TECHNICAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality	Reoccurring or automated recon events. Reoccurring or automated unsuccessful activity events.	Disclosure of network topology or interconnectivity. Significant recon events. Significant unsuccessful activity events. User credentials	Administrative credentials to DoD information networks and ISs are compromised
Integrity	Malicious logic defeated by defense mechanisms. Exposes limited number of ISs or global network services to risk	Propagation of malicious logic that could significantly affect the Department of Defense. Exposes moderate number of ISs or global network services to significant risk. Malicious logic having well-understood capabilities and which will not cause significant damage or loss.	Inability to verify or known modification to highly sensitive DoD intellectual property. Widespread propagation of malicious logic; could significantly affect DoD. Exposes large number of ISs or global network services to significant risk (e.g., 0-day exploit). Malicious logic capabilities that are unknown or not fully understood.

Table D-C-2. Technical Impact Examples

	POTENTIAL TECHNICAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Availability	User workstation is inaccessible.	Degradation of services for day-to-day business. A mail server was removed from the network and users were unable to access mail. User Web portals and Web applications are not available	Degradation or unavailability of DNS, routing, or PKI infrastructure.
All Security Objectives	IS was not patched or protected. Exploitation technique used infrequently. Exploitation of the IS can be conducted locally with physical access.	IS was partially patched and protected. Exploitation technique used frequently. Exploitation of the IS can be conducted remotely or locally with user interaction.	IS was fully patched and protected. Exploitation technique widespread. Exploitation of the IS can be conducted remotely with no user interaction.

Table D-C-2. Technical Impact Examples (continued)

	POTENTIAL OPERATIONAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality	A set of configuration information about an obsolete unclassified IS is found on a NIPRNET account. Old duty rosters or schedules are in an accessible directory	Unauthorized disclosure of technical reporting structures or TDY assignments.	Unauthorized disclosure of highly sensitive DoD Program Information, mission plans or orders, or deployment plans.
Integrity	Access to deployment records for operations that have been completed are found on compromised machine.	Loss of confidence data stored on a MAC II IS for less than 2-3 days. Applying fix to legacy IS based on bulletin or alert leaves application vulnerable to unauthorized access.	IS used to manage aircraft maintenance records compromised. Degradation of services on a MAC I IS.
Availability	Access to files on personnel who are terminated is unavailable. Access to purchasing database for equipment look-ups is offline.	Unable to process TDY orders. Organization is unable to perform effective C2 with its parent / subordinate organization due to a disabled mail server.	Inhibited ability to manage inventory, deliver supplies, or meet deployment timelines.

Table D-C-3. Operational Impact Examples

	POTENTIAL OPERATIONAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
All Security Objectives	Generates limited if any military action. Causes local adverse publicity. Causes limited or localized coverage in news media. Short-term physical injury or harm. Resources required for response will have limited effects on operations and not significantly reduce the effectiveness of response functions.	Affects a MAC III IS, OSD information network, or DoD information network. Generates moderate level of military action. Causes national adverse publicity. Causes moderate coverage in news media. Permanent physical injury or harm. Resources required for response will have moderate effects on operations and may reduce the effectiveness of response functions temporarily.	Affects a MAC I/II IS, classified IS, or guard device. Risk to human life or widespread physical injury or harm. Crosses CC/S/A/FAs boundaries. Impacts operational mission of B/P/C/S level or higher information networks. Generates a higher level of military action. Causes a national reaction. Affects national reaction. Causes widespread coverage in news media. Resources required for response will have significant effects on operations and reduce the effectiveness of response functions for a significant period of time.

Table D-C-3. Operational Impact Examples (continued)

ENCLOSURE E

CYBER INCIDENT RESPONSE

1. Introduction

a. Incident response is an organized and coordinated series of steps, also known as Response Actions (RAs), to resolve or mitigate a reported incident. It also includes the steps taken to recover affected ISs and return them to a fully operational and secure state.

b. Coordination, communication, and documentation actions are also taken during incident response to ensure the right CC/S/A/FAs are involved, notified of the outcomes, and provided any follow-up reports.

c. It is also in this phase that incident information and incident response actions are archived and recorded. Once the incident is resolved, it is closed, a final report is submitted, and any postmortem actions are completed.

d. This section provides further guidance on incident response and recovery. Further requirements shall be articulated in OPORDs issued by relevant commands.

e. The primary objectives for RAs are to:

(1) Halt or minimize attack effects or damage while maintaining operational mission continuity.

(2) Ensure the effective and timely recovery of ISs in a way that prevents similar incidents from occurring again.

(3) Strengthen the Department of Defense's defensive posture and operational readiness.

(4) Ensure that RAs occur in a manner that protects any data according to its level of sensitivity.

(5) Support rapid, complete attack characterization.

2. Types of Responses

a. Three types of response activities can occur:

(1) Technical Response. RAs that involve containment or eradication of any risks or threats associated with the incident, and the rebuilding or restoring of affected ISs to a normal operational state.

(2) Management Response. RAs that require some type of administrative, supervisory, or management intervention, notification, interaction, escalation, or approval as part of any response. Administrative or management response steps can include actions taken by human resources, public relations, financial accounting, audits and compliance, and other internal organizational entities.

(3) LE/CI and Intel Response. RAs associated with LE/CI; liability; privacy issues; creating or reviewing nondisclosures and service level agreements; and any other legal actions taken in response to an incident.

b. RAs across these three areas will be coordinated.

c. CC/S/A/FAs must be prepared ahead of time for any RAs. Decisions made in haste while responding to a critical incident are rarely effective. Therefore, response procedures, tools, defined interfaces, and communications channels and mechanisms will be in place and tested beforehand.

d. Each CC/S/A/FA will develop response guidance or a response plan. The response plan lists steps to take and specifies who should take them. In this way, when an incident does occur, appropriate personnel will know how to respond. Escalation procedures and criteria must also be in place to ensure effective management engagement in RAs.

e. Preparations that will facilitate response activities include:

(1) An archive of boot disks and distribution media for all applications and OSs.

(2) An archive of security-related patches for applications and OS.

(3) Test networks and ISs (to test patches, analyze malicious code, etc.).

(4) A resource kit of tools and hardware devices to support analysis or data acquisition.

3. Developing and Implementing Courses of Action

a. Courses of action (COAs) include the actions necessary to respond to the reportable cyber event or incident, fix the IS, return the IS to operations, and assess the risk for the IS or information network.

b. Those involved in developing COAs will depend on the incident and the affected CC/S/A/FAs. They may be developed by field operations or by CNDSPs, or jointly by both working with any commanders.

c. Who will actually execute the COAs will depend on who has responsibility for various infrastructure components.

(1) COAs may include CND RAs IAW CJCSI 3121.01, "Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces." Analysis, comparison, and selection of the best COA should be done at the lowest command possible, consistent with established C2 of Cyberspace Operations.

(2) COAs may include the development and issuance of bulletins and other notifications to CC/S/A/FAs to promote awareness, direct actions, and ensure compliance.

(3) Those with key roles in responding to an intrusion must be notified and kept informed to fulfill their responsibilities. Executing COAs and information dissemination procedures may include contacting users, security personnel, LE/CI, vendors, Internet service providers (ISPs), other CNDSPs, and other internal or external security organizations.

(4) Specific coordination may be required with DoD LE/CI or with external law enforcement organizations when DoD LE/CI support is not available or cannot be obtained due to time or distance factors. Coordination with LE/CI involves helping LE/CI personnel investigate the incident and prosecute the perpetrators, if warranted.

(5) International coordination may be needed if attacking hosts reside in a foreign nation or if DoD ISs are attacking networks in that nation.

(6) USCYBERCOM reserves the right to direct and assist CC/S/A/FAs with response actions for incidents that fall into a DoD enterprise incident set or when actions otherwise affect multiple theater or Service information networks.

d. For more information on coordination and collaboration with LE/CI and international organizations, see Enclosure F (Collaboration with Other Strategic Communities).

e. NIST SP 800-61, "Computer Security Incident Handling Guide" (reference cc), provides a list of criteria for determining appropriate courses of action or what it calls "strategies." These criteria include:

(1) Potential damage to and theft of resources.

(2) Need for evidence preservation.

(3) Service availability (e.g., network connectivity, services provided to external parties).

(4) Time and resources needed to implement the strategy.

(5) Effectiveness of the strategy (e.g., partially contains the incident, fully contains the incident).

(6) Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in 2 weeks, permanent solution).

f. NIST describes COAs and RAs for various attacks such as DoS, malicious code, unauthorized access, and inappropriate usage in NIST SP 800-61 (reference cc).

4. Recovering Without Performing Technical Analysis

a. Data from all incidents must be preserved to enable technical analysis. However, under certain circumstances and with approval, technical analysis may not be required prior to IS recovery.

(1) For example, it may not be possible to conclusively identify the root cause of an incident through additional analysis. The intruder may have deleted or tampered with logs and files, making them untrustworthy. The existence of multiple unpatched vulnerabilities may make it impossible (or not worth the effort) to try to identify which specific vulnerability was exploited. In such cases, it may be more expedient to begin IS recovery and hardening.

(2) Potential technical and operational implications should be assessed carefully prior to recovering an IS without performing technical analysis. Such an assessment will indicate how this may impact mission success. For example, the primary benefit of determining root cause and eradicating it prior to redeploying an IS is to prevent similar system compromises and to share that information with other DoD communities, thereby strengthening the overall security posture of DoD information networks. If a root cause is not identified and eradicated, the IS may once again be compromised and others may lose the valuable information provided by the technical analysis.

5. Containment

a. Overview

(1) Containment consists of short-term, tactical actions to stop an intruder's access to a compromised IS, limit the extent of an intrusion, and prevent an intruder from causing further damage.

(2) The primary objectives for containment are to:

(a) Regain control of the ISs involved in order to further analyze the cyber incident and return the IS to normal operation.

(b) Deny an intruder access to prevent him or her from continuing the malicious activity and from affecting other ISs and data.

(3) While an intruder has access to an IS, the IS cannot be properly analyzed or restored. Performing containment:

(a) Prevents an intruder from accessing or exfiltrating DoD data or other information.

(b) Prevents an intruder from destroying valuable evidence and tampering with ISs while they are being analyzed.

(c) Prevents an intruder from using DoD ISs to attack other ISs, protecting the CC/S/A/FAs from liability.

(4) Containment provides a reasonable security solution until sufficient information has been collected to address the vulnerabilities exploited and the damage sustained.

(a) It should be noted that some containment actions can be taken during the preliminary response phase of the incident handling life cycle.

(b) More containment steps may be warranted following in-depth analysis, which may identify more affected ISs or malicious activities. Containment steps can be executed iteratively with the steps in the detection and analysis phase.

(5) Containment strategies are executed by the CC/S/A/FA responsible for the maintenance and operation of the affected DoD information networks or ISs, this could be a local system administrator or could be the component's CNDSP. Who executes the strategies will depend on the incident type, affected component, and local policy and procedures.

b. Containment Strategies. Containment strategies will vary based on the type of incident. Containment activities may include any of the following, or any other strategies determined by the affected CC/S/A/FAs.

(1) Blocking. Blocking is the use of network access controls at the perimeter or enclave boundary to prevent the attacker from connecting to other DoD information networks, ISs, or DoD data and services.

(a) The decision to block is based on the incident category, the threat to the network, and instruction from CI/LE and USCYBERCOM.

(b) Category 1, 2, 3, 4, 6, and critical 7 incidents require immediate blocks at the host and/or gateway level if the risk of further compromise, data exfiltration, and continued threat to the DoD information networks outweighs the benefit of monitoring adversary TTPs for a more comprehensive countermeasure.

(c) Other incident categories, such as 5 and 8, may elicit a block if the result reduces risk and exposure to potential delivery vectors.

(d) Block requests will include inbound and outbound traffic.

(e) Border Gateway Firewall Block. Gateway IP and port blocks are used to prevent the spread of compromise from an identified external IS or delivery vector. Category 1, 2, 3, 4, 6, and 7 incidents could necessitate gateway blocks. Block requests will include inbound and outbound traffic. Sample blocks include:

1. IP addresses that host malicious code, malware, spyware, or unauthorized software.

2. Peer-to-peer (P2P) and instant messaging (IM) communication ports.

3. Mail relays, phishing, and spam originators.

4. Known hostile IP addresses and hosts.

5. IP addresses and ports associated with worms, botnets, and trojans.

6. External hosts that are identified performing scanning, footprinting, or attempting to exploit DoD assets.

7. DoS attacks.

(f) Enclave Firewall Block. Enclave firewall blocks follow the same process as gateway blocks depending on the scope of the incident. Enclave blocks are specific to the component behind the firewall. Block requests will include inbound and outbound traffic.

(g) Mail and Proxy Block. Mail gateway blocks are required when e-mail is the identified delivery vector. Mail blocks include filtering for attachments, subject lines, and senders. Examples include spam, phishing, worms, and other mail attachments attacks containing malicious code. Proxy blocks are dependent on the content filtering solution of the component managing the proxy application.

(2) Network Isolation. Network isolation involves the use of network access controls to logically segment the network and restrict access to the affected hosts. Isolation strategies include the following:

(a) Disconnect the IS From Any Local Area Network. This will help prevent further contamination of the affected information network and IS.

(b) Disconnect IS From the Internet or Any Other Public Networks. This will help to prevent inbound access or outbound traffic or data exfiltration.

(c) Disconnect or Isolate the Affected Network Host and/or Segment from the Rest of the Network. This can help to prevent further contamination or containing malicious activity to an IS or logical network segment. This will allow attached ISs to still function but will not spread malicious activity to the rest of the infrastructure. In some cases, this may be relevant to monitor adversarial activity while limiting the adversary's ability to attack other ISs.

(3) IS, Server, or Service Shutdown. Shutting down an IS, server, or service may help limit damage or prevent further access to the IS by the adversary. However, it will also affect the ability to acquire certain valuable data for the incident analysis. The decision to pursue this containment strategy should be weighed carefully.

(a) IS Shutdown. If it is determined that allowing the IS to function will destroy data or applications on the IS, the IS should be shut down with the commander's approval as a containment measure.

(b) Server Shutdown. If it is determined that a particular server, such as an e-mail or Web server, requires shutdown until problems can be eliminated or to contain the spread of malicious code, the specific server should be shut down. Be advised that in addition to destroying non-volatile data, shutting down a server may adversely affect multiple users and mission operations. This decision should be made in coordination with the relevant command authority.

(c) Service Shutdown. If sufficient analysis has been performed to correctly limit the scope of an intrusion to specific services, these services can be disabled (especially if no patch is available). Be advised that in addition to potentially destroying non-volatile data, shutting down a service may adversely affect multiple users and mission operations. This decision should be made in coordination with the relevant command authority.

(4) Other Containment Strategies. Other containment strategies presented by NIST 800-61 (reference cc) include the following:

(a) Eliminate the attacker's route into the environment by preventing attacker from accessing nearby resources that might be targets.

(b) Block the transmission mechanisms for the malicious code between infected ISs.

(c) Disable user accounts that may have been used in the attack.

c. Temporarily Leaving IS Online

(1) Under certain circumstances, the commander may decide to leave the affected IS online and accept the risk in operating in and through a compromised environment based on operational requirements. Additionally, the commander may decide to leave the affected IS's vulnerability accessible in order to monitor the attacker's activities.

(a) CNDSPs will monitor an attacker's activities at all times regardless of LE/CI involvement. This monitoring for IS protection purposes is conducted in the ordinary course of business and authorized by federal law. The results of monitoring for network defense may be shared with LE/CI organizations 18 U.S.C. 2511(2)(a)(i) (reference dd).

(b) CNDSPs are not authorized to conduct monitoring on behalf of LE/CI organizations for purely LE/CI purposes unrelated to CND. LE/CI organizations must consult their servicing Staff Judge Advocate (SJA) about monitoring.

(2) If a compromised IS is left running, NIST recommends, "management and legal counsel should ensure there is no liability that can result." NIST also cautions "not containing malicious activity can cause more

malicious activity to occur because malicious code or actions continue which can cause further damage and loss of operations or DoD data."

d. Caveats for Containment

(1) Any changes to compromised ISs, including containment actions, may destroy information required to assess the cause of an intrusion. Ensure that all necessary data for analysis is completely collected before making any IS changes. Also, collect and protect all evidence that may be needed in a subsequent investigation before performing any containment actions.

(2) CC/S/A/FAs and CNDSPs must define acceptable risks for incident containment and develop strategies and procedures accordingly.

(3) Various questions arise when deciding whether to contain malicious or unauthorized activity. Answers to these questions may require discussions with IS and business process owners. Such questions can include:

(a) Is it appropriate to shut down or disconnect an IS?

(b) Does the CNDSP or local system administrator have the authority to shut down or disconnect an IS?

(c) When must an IS stay up and running?

(d) What ISs cannot be taken offline or disconnected?

(e) Are there investigative or intelligence equities to consider? (See Enclosure F.)

(4) Decide appropriate containment strategies for critical assets ahead of time. By preparing in this way, a decision does not have to be made about what is a correct or approved containment strategy during an incident.

(5) If the intruder's actions are rapid and spreading, system administrators and CNDSPs may need to take more immediate action; response and containment policies and procedures should contain guidance for such situations.

6. Eradication

a. Overview

(1) Eradication consists of the steps required to eliminate the root cause(s) of an intrusion. All threats and risks should be removed from DoD

information networks and ISs before returning them to service. If the threat is not removed, then an IS can be easily compromised or breached again.

(2) The primary objectives for eradication are to:

(a) Ensure the removal of the cause(s) of the malicious activity and any associated files.

(b) Ensure the elimination of any access methods used by the intruder, including vulnerabilities, physical security problems, or human error.

(3) Execute eradication steps after the first round of containment actions occur and then interactively with any further analysis and containment activities.

(4) Sometimes, full eradication can only happen after long-term policy and configuration management changes are put into place. In that case, the threat should be mitigated to the extent possible before rebuilding and reconnecting any affected ISs.

(5) Some ISs, due to the nature of the incident, may not need any eradication steps, or the eradication may occur as part of the recovery activities when the infected IS is wiped or erased and rebuilt.

(6) Eradication strategies are executed by the CC/S/A/FA responsible for the maintenance and operation of the affected information networks or ISs; this could be a local system administrator or could be the components CNDSP. Who executes the strategies will depend on the incident type, affected component, and local policy and procedures.

b. Eradication Strategies. Specific eradication actions depend on the nature of the incident.

(1) Remove Malware. Quarantine, delete, replace, or restore the integrity of infected files. In most cases, this will require rebuilding the IS from trusted media. This may also involve updating antivirus signatures.

(a) Under most conditions, once an IS is compromised the integrity of that IS cannot be verified until it has been restored from trusted media. If a IS contains malware, keeping it in operation is not recommended unless the complete integrity of that IS can be once again verified, or the IS is left running and monitored closely as part of an ongoing LE/CI case. In the latter case, the decision to leave the IS running must be based on approvals by authorized DoD personnel.

(b) Any malware uncovered throughout the incident response process must be cataloged in the JMC. Additional guidance may be found in Enclosure G (CND Incident Handling Tools—Joint Malware Catalog).

(2) Remediate or Mitigate Vulnerability. Remove vulnerabilities by installing any new operating IS or application patches to vulnerable software to prevent exploitation. If the IS cannot be patched for technical or operational reasons, mitigate the vulnerability by updating IS configurations and defenses to protect or segment the affected host. If a patch is not available, apply workarounds or temporary mitigation strategies.

(3) Modify Access Controls. Update user and network access controls. For instance, remove compromised user or administrator accounts; modify network access controls (e.g., IDS/IPS, firewall, content filtering); update baseline configurations; and remove any other access mechanisms used by the adversary.

7. Recovery

a. Overview

(1) Recovery consists of the steps necessary to restore the integrity of affected ISs, return the affected data, ISs, and information networks to an operational state, and implement follow-up strategies to prevent the incident from happening again.

(2) The main objectives of recovery are to:

(a) Restore the integrity of the IS by rebuilding it from trusted media when necessary.

(b) Implement proactive and reactive defensive and protective measures to prevent similar incidents from occurring in the future.

(c) Ensure all data and ISs are operating in a normal fashion.

(d) Ensure the complete resolution and closure of the incident.

(3) Data and ISs are fully restored when the necessary patches and fixes applicable to the incident have been installed. If an IS is compromised, the integrity of anything on that IS is suspect. The intruder could have changed the kernel, binaries, data files, running processes, or memory. The only way to be sure an IS is free of malicious code and back doors is to reinstall the trusted media and then install any security patches and upgrades. This includes both OS and application patches.

(4) Also, as part of the recovery process, any containment activities completed may need to be removed. This can include removing any blocks that are no longer necessary, re-enabling services, and reconnecting ISs and information networks to the LAN or Internet.

(5) Recovery strategies can be executed by a variety of DoD personnel based on their roles and responsibilities. Multiple strategies may need to be implemented across the affected component. Who executes the strategies will depend on the incident type, affected component, and local policy and procedures.

b. Recovery Strategies. Depending on the nature of the incident, recovery actions can include, but are not limited to the following:

(1) Rebuild from Trusted Media. Reinstall the OS and applications from a trusted backup, or from original distribution media.

(2) Verify System Data. Review IS data to ensure its integrity. Someone who knows what user or other data was on the IS should review the data to ensure it has not been changed. Alternatively, restore IS data from a trusted backup.

(3) Change System Passwords. Change all passwords on the IS and possibly on all ISs that have trust relationships with the victim IS.

(4) Improve Network and Host Security

(a) Increase host and network monitoring.

(b) Enable maximum host logging, auditing, and accounting programs.

(c) Disable unnecessary services.

(d) Verify there are no weaknesses in configuration files for those services.

(e) Install all the latest vendor security patches and upgrades if approved and tested.

(f) Update firewall rule-sets.

(g) Update boundary router ACLs.

(h) Update IDS/IPS signatures.

(i) Review any DoD guidance, advisories, or bulletins to see if there are other recovery actions or security enhancements that can be enabled or installed.

(j) Install new security mechanisms that may help protect ISs or detect malicious activity. This can include programs like file integrity checkers, URL checkers, etc.

(k) Implement any needed mail filtering.

(l) Update any security policies to reflect or support these security improvements.

c. Once all recovery steps have been completed and ISs have been tested to ensure they are operating normally, reconnect any hosts or information networks that were disconnected.

(1) All ISs that have a Category 1, Category 2, or Category 7 incident must be erased and rebuilt from trusted media, then patched and updated prior to connecting the IS to the information network. This is necessary to prevent an incident from recurring.

(2) Mission impact may require the affected vulnerable component be mitigated temporarily until the mission allows the IS to be rebuilt. For other categories, CC/S/A/FAs have the discretion of rebuilding the IS depending on the impact of the incident.

(3) STIGs and technical configuration data are provided as required from DISA Information Assurance Support Environment (http://iase.disa.mil) and NSA security configuration guides (http://www.nsa.gov/snac).

(4) CC/S/A report compliance status or directed action of each task or action via Vulnerability Management System (VMS) for their ISs and assets. By doing so, USCYBERCOM and each Combatant Command has visibility of the compliance status of all Service and agency assets that support the Combatant Command.

8. <u>Post-Incident Activity</u>

a. <u>Overview</u>

(1) One of the final parts of the incident handling process is learning how to improve operations, processes, and infrastructure defenses by reviewing

the incident and the response. A postmortem is a review of the incident, including the detection, analysis, and response phases.

(2) The primary objectives for performing a postmortem include:

(a) Identifying infrastructure problems to be addressed.

(b) Identifying ISs and configurations weaknesses or other vulnerabilities to be corrected.

(c) Identifying organizational policy and procedural problems to be reviewed and addressed.

(d) Identifying technical or operational training needs.

(e) Determining unclear or undefined roles, responsibilities, interfaces, and authority.

(f) Improving tools required to perform protection, detection, analysis or response actions.

(3) The CC/S/A/FA with primary responsibility for handling the incident will normally take the lead in performing the postmortem and collecting and trending any outputs. However, in certain circumstances a management, audit, or other group may coordinate this, as appropriate.

b. Post-Incident Activity Strategies

(1) Results from a postmortem shall be used to make improvements to the incident management process and methodology along with any improvements to the security posture and defenses of the CC/S/A/FAs critical to achieving the mission of the DoD.

(a) CC/S/A/FA HQ will establish a formalized postmortem process and establish criteria defining which incidents require postmortems. Not all incidents may require a postmortem. Incidents that are large in scope, handled poorly, involve law enforcement, or caused severe damage are candidates that require a postmortem. Less severe incidents such as regular scanning require a limited postmortem or no postmortem.

(b) All parties involved in the incident should be part of the postmortem. A postmortem shall be held as soon as possible to answer questions such as the following:

1. What were the timeframes for the incident, its detection, and its resolution?

2. What actions were correctly executed by users, analysts, and management, and what actions were not correctly executed?

3. Were appropriate procedures available and followed? Were they up-to-date and correct? Were they still applicable?

4. What would the staff and management do differently the next time a similar incident occurs?

5. What corrective actions can prevent similar incidents in the future? This should include recommendations for signature updates and/or development and changes to ACLs, filters, and system configurations.

6. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

(2) Pertinent information resulting from the postmortem should be added as part of the final report for the incident.

(3) New or unusual cases can be captured and used as the basis for future training exercises or case studies.

(4) After the postmortem is completed, feedback on improvements to be made to policies, procedures, and infrastructure defenses should be passed to the appropriate CC/S/A/FA responsible for making those improvements, provided there is support and approval from commanders and HQ. It is important to implement any changes that can be made based on these lessons learned. This will help provide a more effective defense against recurring or similar incidents. Changes to be implemented can include enterprise or local:

(a) Updates to security policies and implementation guides (e.g., DISA STIGs).

(b) Changes to incident management and incident handling processes and procedures.

(c) Updates to detection systems.

(d) Improvements in IS and information network configurations.

(e) Changes to configurations and filters on network perimeter devices, such as firewalls, routers, and gateways.

(5) The postmortem analysis and lessons learned produce information and incident data that can be collected and used in various ways. This information can be used to create baselines for benchmarking performance, timeliness, and types of incidents seen. It can also be used to generate trending and correlation information for historical purposes to determine whether response actions are actually resolving problems over time.

(6) Data to collect and trend can include but is not limited to:

(a) Recurring problems and recurring user errors.

(b) Incident costs including damage sustained and response and recovery efforts.

(c) Incident precursors.

(d) Types of incidents seen over time.

(e) Types of weaknesses exploited (e.g., certain applications, OSs, social engineering tactics).

(7) Output from postmortem analysis and lessons learned can also be used as case studies and training materials for new staff.

(

ENCLOSURE F

COLLABORATION WITH OTHER STRATEGIC COMMUNITIES

1. Introduction

a. It is in the long-term interest of the Department of Defense to gain attribution and prosecute malicious individuals attacking DoD ISs. The DoD CND community works hand-in-hand with the DoD LE/CI to investigate and monitor individuals who attack DoD ISs. Information and insights gained from investigations can then be provided back to the DoD community to increase the overall defensive posture of DoD information networks.

b. All unauthorized access to information networks or ISs is considered punishable as a crime. The DoD investigative agencies conduct LE/CI investigations and operations in support of CND. In doing so, the DoD investigative agencies obtain and provide relevant threat data for use in mitigating threats to the DoD information networks.

c. The success of DoD CND response depends on the Department of Defense's ability to effectively share and fuse analytical and operational information across and within organizational boundaries, including operational components, service providers, and the LE, CI, and intelligence communities in a timely manner. This enables improved battlefield awareness across the full spectrum of military operations to accurately characterize and understand the effects of network intrusions on DoD information networks and to improve military decision making about response strategies.

2. Operational Cooperation with LE/CI

a. Reporting incidents and sharing information, notifications, and coordinating analysis of security incidents with DoD investigative agencies facilitate criminal attribution in the event U.S. code has been broken. The DoD investigative agencies obtain and provide relevant threat data in a timely manner to mitigate threats to the DoD information networks. The focal point for Net Defense threat data in the Department of Defense is USCYBERCOM.

b. Deconflicting Investigative Actions. In some circumstances, LE/CI may request DoD IS providers to allow a potentially compromised DoD IS to remain operational for the purpose of facilitating LE/CI investigations and operations. The commander of the organization shall make every effort to support such requests; however, commanders are still required to maintain and defend their operations and, ultimately, the information networks that facilitate those operations. Additional information can be found in Appendix A to Enclosure F (Coordination and Deconfliction).

c. When investigative actions conflict with protective measures, these measures will be coordinated with the affected investigative service ahead of time unless there is an imminent threat.

(1) Supporting the Legal Process. Commanders must be careful to balance short-term requirement to conduct operations with the long-term advantage of prosecuting malicious individuals. If a commander is notified of a legal process, such as a subpoena or warrant, has been issued and that their actions may conflict with the intent of that order, the commander will coordinate with LE/CI and the servicing SJA on any actions so that a legal process is not obstructed. Commanders will also promptly inform the USCYBERCOM SJA of any potential conflict.

(2) Data and Information Management. Actions required supporting LE/CI investigations may include, but are not limited to, copying device media to facilitate media analysis.

(a) Care should be taken in the release of device storage media images or the results of analysis. Media is classified to the highest level of information contained on the media. Additionally, the data on the media may be sensitive but unclassified, such as CUI, limiting its sharing outside the Department of Defense.

(b) If the device is evidence in an LE/CI investigation, the media may be LE/CI sensitive, requiring special handling and a law enforcement sensitive (LES) caveat. While this does not forbid CND analysts from performing technical analysis, special care shall be taken to ensure the dissemination of analytical results does not compromise an LE/CI investigation. The commander of the organization shall coordinate with LE/CI when releasing such information.[9]

(c) The operational community and LE/CI organizations must effectively collaborate in order to rapidly disseminate information necessary for network defense while minimizing the potential for compromise of LE/CI operations, sources, and methods. Many times this can be done effectively through the use of “tear lines,” etc.

[9] Where applicable, it may be more convenient to separate these concerns by using two system images: one image for CND purposes and one image for LE/CI purposes.

(3) Sharing Information. Trust must be established and maintained among the numerous LE/CI agencies. Although there may be no legal restriction on sharing certain information, for instance in regard to an ongoing operation, many agencies may be hesitant to share information that could jeopardize the safety of their sources, methods, and agents. Although information obtained by the LE/CI community is governed by unique restrictions and considerations, if this information is important to the security of DoD ISs, it can be shared with appropriate controls and limitations on distribution. To improve the flow and timeliness of the threat information obtained by the LE/CI community, both the DoD CND organizations and the LE/CI community must ensure formal processes are established to improve mutual understanding of one another's needs, capabilities, and unique restrictions.

d. LE/CI Threat Data

(1) From a CND perspective, the principle value of the LE/CI community is the threat information it obtains through investigations and operations. Threat data consists of information that can help lead to increased defense of DoD information networks and the attribution and intent of network intruder(s). It can consist of planned actions that could adversely affect DoD ISs. Threat data also consists of specific methodologies (toolsets, techniques, targeted vulnerabilities) used by network attackers that are discovered through an investigation.

(2) Typical sources of data include:

(a) Logs and records of ISPs recorded during the course of an intrusion, as well as those ISP records used to store hacking tools, stolen data, e-mails, chat rooms, etc.

(b) Information sharing with local, state, federal, and international law enforcement counterparts.

(c) Interviews of human sources in support of proactive operations and reactive investigations.

(d) Wiretaps, pen trap, and trace, etc.

(3) In addition to developing threat data during an investigation or operation, the LE/CI community deters future threats by enforcing various statutes and prosecuting those who violate the law.

(4) The CI community offers various capabilities and options when countering the activities of foreign intelligence services and international terrorists.

(a) Insider Activity. 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.

(b) Unique Restrictions on Law Enforcement Data. As noted above, the network defense can gain very important information from LE/CI investigation and/or operations; however, much of the information may require LES controls.

3. International Coordination

a. International coordination and collaboration are achieved in a number of ways. The Department of Defense has established relationships with many countries through specific bilateral and multinational agreements (for instance, CND information sharing with the 5 Eyes CND community is conducted by USCYBERCOM (J3) under the auspices of the International CND Coordination Working Group). Information is shared routinely, to generate shared situational awareness amongst allied and partner nations, but coordination and collaboration may also occur in response to specific incidents.

(1) The USCYBERCOM J3 functions as the focal point for DoD communications with allied military counterparts. USCYBERCOM will coordinate with Geographic Combatant Commands of agreements with allied military counterpart organizations in their AOR.

(2) Geographic Combatant Command international CND coordination and collaboration will occur under predefined agreements with military forces, nations, or international organizations in their AOR.

b. In extremis, there may be a need to coordinate quickly with other foreign countries in which attacking hosts reside. Existing relationships and arrangements will be used to the greatest extent practicable according to the extent to which they may be beneficial.

c. The key questions that may need to be addressed include:

(1) What is the state of relations between the United States and the nation in question?

(2) Will a request for assistance itself constitute a greater threat to national security than the attack or intrusion itself? This includes an assessment of whether the country is an actual sponsor of the attack or may

gain valuable information that could be used to attack the Department of Defense.

(3) Does the nation in question have the technical capacity to respond to a request for assistance?

(4) How long will it take for the nation to act on the request? Is that too long given the threat to national security?

d. The IC has multiple vehicles for working with its counterparts in allied countries. These relationships have a proven history of quickly tipping the allied countries, and vice versa, to threat activity, providing new indications and threat vectors, and increasing information sharing. The USCYBERCOM J2 and/or the appropriate GCC J2 DoD Intelligence Agency will act as the focal point for operational intelligence requests to Allied or foreign partner CND intelligence organizations through existing information sharing agreements.

e. The LE/CI community has a long history of working with its counterparts in allied and other foreign countries. The LE/CI organizations at USCYBERCOM will serve as the repository for relevant information shared by the LE/CI community, conveying CND organization requests for information to the LE/CI community and providing a focal point for LE/CI coordination with USCYBERCOM.

f. In cases where international coordination is required beyond the capabilities of the USCYBERCOM and LE/CI community, USSTRATCOM will forward a request to the Department of State via the Secretary of Defense.

4. Intelligence Community

a. Intelligence support to CND is essential to provide knowledge, reduce uncertainty, and support effective operational decision making. According to the definition of CND found in DoDI O-8530.2 (reference c), CND " . . . employs intelligence, counterintelligence, law enforcement and other military capabilities to defend DoD information and computer networks."

b. Accurate and timely intelligence analysis of network events and of adversaries' actions against the Department of Defense's enterprise is critical to ensuring operations and the future viability of the military's vital information resources and investments.

c. The Intelligence Support to CND offices provides all-source intelligence in support of their respective organizations' priority intelligence requirements. All source intelligence consists of information that can help lead to increased defense of DoD information networks and attribution and intent of network intruder(s). It can consist of planned actions that could adversely affect DoD

ISs. All-source intelligence also consists of specific methodologies (toolsets, techniques, targeted vulnerabilities) used by network attackers.

d. Each CNDSP is responsible for, and should identify processes for working with, their appropriate Intelligence Support Element. This relationship will vary based on organization and internal authorities and requirements, but can provide a wealth of threat data, indications and warning, and the ability to query the national level IC. Technical reporting between incident handling program and intelligence is maintained in the JIMS. JIMS is the Department of Defense's new central repository for this key intelligence. The primary objective of the database is to ensure the timely flow of crucial network intelligence across DoD/USG and ally boundaries.

e. For additional guidance, see Appendix B to Enclosure F (Intelligence Support to Incident Reporting).

5. Cyber Unified Coordination Group. The Cyber Unified Coordination Group (CUCG) consists of senior representatives from federal agencies that have roles and responsibilities related to preventing, investigating, defending against, responding to, mitigating, and assisting in the recovery from cyber incidents and attacks.[10] The CUCG is responsible for the following:

a. Provide input to member agencies and department heads and the Interagency Incident Management Group (IIMG) on cyber security issues, incidents, and threats.

b. Assist in reviewing threat assessments and providing strategic situational awareness and decision support across the national cyber incident management spectrum, including prevention, preparedness, response, and recovery.

c. Integrate information, frame policy issues, and recommend actions—including use or allocation of federal resources—for agency and department heads, the IIMG, and other appropriate officials.

d. Coordinate with the DHS National Operations Center to disseminate critical information to and from government and non-government sources, such as information sharing mechanisms, academia, industry, and the public.

e. Support the Executive Office of the President, as appropriate.

[10] The NCRCG is an interagency forum where organizations responsible for a range of activities (technical response and recovery, LE, intelligence, and defensive measures) coordinate for the purpose of preparing for and executing an efficient and effective response to an incident.

APPENDIX A TO ENCLOSURE F

COORDINATION AND DECONFLICTION

1. Introduction

a. Coordination and deconfliction 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.

b. For the purpose of this guidance, coordination and deconfliction 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) Deconfliction is a subset of coordination in which information is shared to eliminate overlap or interference between ongoing activities.

2. Types of Operations

a. Time-Sensitive Operations. Time-sensitive operations generally involve network-centric COAs to defend the DoD information networks against imminent or ongoing threats.

(1) 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.

(2) As a general rule, inputs for time-sensitive operations will be required from all organizations within 4 hours of notification by USCYBERCOM.

(3) USCYBERCOM J2 will manage requests for IC coordination and deconfliction with the appropriate IC members. The LE/CI organizations (at USCYBERCOM) shall conduct LE/CI coordination and deconfliction with appropriate LE/CI organizations.

(4) Organizations participating in the coordination and/or deconfliction 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 in accordance with this manual.

b. Non-Time-Sensitive Operations. Non-time-sensitive operations are network-centric and non-network-centric COAs to defeat or mitigate ongoing threats such as a persistent, sophisticated intruder.

(1) While coordination and deconfliction 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.

(2) Non-time-sensitive coordination and deconfliction will use a more deliberative process employing periodic coordination and/or deconfliction meetings, correspondence, teleconferences, and video teleconferences.

(3) Non-time-sensitive coordination and deconfliction 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.

(4) Coordination and/or deconfliction 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.

c. Operational Practices. Coordination and deconfliction must occur across tiers, between agencies, and with other DoD or external organizations, as appropriate. The following operational practices provide guidance on how this should occur.

(1) Establishing Meeting Frequency. Determine how often coordination and deconfliction actions must occur between organizations.

(a) For Tier I level incident responses, USCYBERCOM will establish the coordination/deconfliction meeting frequency and ensure meeting notification is provided to appropriate organizations.

(b) For Tier II level responses, the respective CC/S/A/FA will establish the coordination/deconfliction meeting frequency and ensure meeting notification is provided to appropriate organizations, keeping USCYBERCOM informed of any planned and executed incident responses.

(2) Initial Notifications. Initial notification and request for coordination and deconfliction shall include the following information (at a minimum):

(a) A summary of the CND event, to include: threat assessments, damage assessments, technical and operational impacts, and actions taken.

(b) Attribution assessment with levels of confidence.

(c) COAs under consideration and assessment.

(d) Time when inputs must be provided back to the incident response lead agency.

d. Managing Concurrence and Alternative COAs. Work with all parties affected by the response to understand their level of concurrence with the recommended COAs and to solicit alternative COAs as needed.

(1) Coordination and/or deconfliction inputs from the IC or LE/CI organizations for both time-sensitive and non-time-sensitive operations will include a statement of understanding, where they may concur or nonconcur with proposed COAs.

(2) In cases where an organization nonconcurs, the organization will provide supporting technical, operational, or policy information as required so the operational impact of COAs on those organizations can be balanced against the ongoing threat. Nonconcurrence does not equate to a veto.

(3) Organizations may recommend alternate COAs in cases where an organization nonconcurs with proposed COA. Organizations may provide assessments of the threat, potential collateral damage, operational impact, and political impact assessment for each COA. Organizations may also recommend no action be taken for DoD, allied, and other forces networks.

(4) Organizations should identify data discrepancies and corrected data if they do not concur in that data provided by the incident response lead agency.

(INTENTIONALLY BLANK)

APPENDIX B TO ENCLOSURE F

INTELLIGENCE SUPPORT TO INCIDENT REPORTING

1. Introduction. Intelligence support to CND is essential in order to provide knowledge, reduce uncertainty, and support effective operational decision-making. Accurate and timely intelligence analysis of network events and of adversary's actions against the Department of Defense's enterprise is critical to ensuring both operations and the future viability of the military's vital information resources and investments.

2. Joint Incident Management System (JIMS)

a. The JIMS is the Department of Defense's central repository for managing event and incident reports. The primary objective of JIMS is to ensure the timely flow of crucial network intelligence across DoD/USG and ally boundaries to reflect the collective reporting of adversary actions, intentions, and capabilities; to assist in shaping tactical, strategic, and military response strategies; and to perform trending analysis, correlation, and fusion.

b. The JIMS is used for recording possible foreign activity and domestic initiated threat activity suspected of being foreign in origin and against DoD networks. Use of the JIMS is required by the USCYBERCOM J2 and each Service component CERT/CIRT intelligence support element for the following categories of intrusions:

(1) Category 1—Root Level Intrusion.

(2) Category 2—User Level Intrusion.

(3) Category 4—Denial of Service.

c. The JIMS may also be used by Combatant Command Joint Intelligence Centers/Joint Analysis Center/Joint Intelligence Operation Centers (JICs/JAC/JIOCs), DIA, NSA, and DoD Service/agency intelligence centers.

d. The JIMS contains incident records based on JIMS entries corresponding to threat activity against DoD computers and information networks. Records include both technical and intelligence data related to the IP addresses conducting activity against DoD ISs.

(1) JIMS will be the primary repository of intelligence related to Category 1, Category 2, and Category 4 incidents and database intelligence related to named intrusion sets. USCYBERCOM J3 is responsible for DoD-focused operations, such as official named intrusion sets.

(2) During analysis of network events, a serious pattern or series of events may be identified and analytically developed by a Service or other element. For the purposes of analytic collaboration and communication, identifying this activity by a specific name may be warranted. In such a case, the Service that identifies the activity will maintain the criteria and determination of what falls into that "named area of interest" (NAI). If the activity crosses multiple services or organizations, USCYBERCOM J3 may determine the activity warrants being an enterprise event. USCYBERCOM may then use the Service's criteria to create an official USCYBERCOM Focused Operation.

(3) The objective of JIMS intelligence reporting is to share intelligence information and events in support of CND by enabling rapid cross-cueing of threat activity and fusion of all-sources of information on foreign threats to DoD information networks.

3. Intelligence Reporting Procedures

a. CND intelligence reporting on network events focuses on foreign threats to DoD information networks and has been divided into three types of reporting.

(1) JIMS. JIMS intelligence reports generated in a timely manner for incidents/events meeting a specified reporting threshold, based on technical event data augmented with all-source intelligence information.

(2) Network Intelligence Report (NIR). All-source intelligence reports focused on details of individual activity or a single event, a correlation of several JIMS incident records, entity reporting on a person or organization related.

(3) Strategic-Level All-Source Intelligence Analysis and Production. DoD intelligence production will produce CND-related intelligence assessments in response to specific consumer requirements and IAW individual organizational production priorities.

b. Initial Intelligence Reporting. Individual incident records in the JIMS are based on threat activity against DoD information networks that might be of foreign origin. Note the JIMS also contains records of domestic IP addresses, but the events associated with this activity are presumed foreign, until proven otherwise.

(1) JIMS records are a timely technical summary of an event supplemented with intelligence analysis that is entered into the JIMS.

Technical event details are derived from an entry in the JIMS or through other sources. Technical specificity in initial JIMS reports is vital to establishing or ruling out correlation between events during follow-on analysis.

(2) A JIMS entry is required for every Category 1—Root Level Intrusion, 2—User Level Intrusion, 4—DoS, and incidents that appear to be associated with USCYBERCOM-focused operations. A JIMS entry for other incident categories is optional, but it is recommended when associated with focused operations.

(3) Input into JIMS of initial analysis is required as soon as information becomes available. Initial analysis on an event should occur as soon as feasible.

(4) The USCYBERCOM J2 and the Service component CERT/CIRT intelligence support elements are required to perform initial JIMS intelligence reporting.

c. NIRs. NIRs can be based on patterns that emerge from correlation of JIMS reports and/or provide correlated and amplifying intelligence on cyber event(s) or entity(s).

(1) There are generally two types of NIRs:

(a) Event-Based NIR. Event-based NIRs focus on an incident, group of incidents, or network activity.

(b) Entity-Based NIR. Entity-based NIRs focus on an individual, group, or organization identified as a threat or potential threat to DoD information networks.

(2) As with initial reports, timeliness for NIRs is important. Upon recognition of a correlation among network incidents, malicious network activity, and analysis on an entity, a NIR should be issued as soon as feasible.

(a) NIRs will be disseminated through message traffic, when organizational processes allow, with a URL link to report if appropriate.

(b) NIRs will have a standard Title/Subject line. Example: "Service/Organization Network Intelligence Report, Serial Number: Title."

(c) The USCYBERCOM and the Service component command CERT/CIRT intelligence support elements are required to perform follow-on reporting when significant patterns or intelligence is identified associated with events or entity activity. NIR reporting may also be generated by Combatant

Command JICs/JAC/JIOCs, DIA, NSA, NGA, and DoD Service/agency intelligence centers.

(d) NIRs will be in following format (Table F-B-1):

SERVICE/ORGANIZATION NETWORK INTELLIGENCE REPORT, SERIAL NUMBER: “TITLE” Summary: Executive overview, key points, and bottom-line. Details: Result of incident, source characterization, target characterization, activity/pattern characterization, and background/entity characterization. Threat Assessment: Analyst comments, recommendations, intelligence impact, OPSEC analysis and significant information from operations. References: Sources used in the report will be included in the Reference section, to include JTID numbers when appropriate. Contact information: Your contact information (organization, e-mail, phone number, etc). Amplifying or Additional Information: When amplifying information exists, it should be included. Examples of this type of information include, but are not limited to, additional technical data, list of hostile IPs, list of victims, signatures, hashes, tools, host names, URLs, intelligence gaps and related collection requirements with appropriate classification markings.

Table F-B-1. NIR Report Format

d. Strategic-level, all-source intelligence analysis and production are also used to satisfy CND intelligence requirements.

(1) Intelligence reporting to the CND community provides the following benefits:

(a) Reports on final attribution.

(b) Provides full-scope examinations of events and incidents.

(c) Provides assessment of event/entity’s and incident strategic significance.

(d) Provides damage assessments.

(2) SIRs may omit the detail provided in initial reports or follow-on reports. These reports should attempt to capture the full military and/or

political significance of network activity. Strategic reporting is normally generated in response to intelligence consumer production requirements based on organization production priorities and focus.

(3) Strategic reports may be based on a wide variety of reporting topics relevant to entities or issues of importance to intelligence support to CND. For example, these reports may provide potential threat information on foreign actors (e.g., governments, sub-national actors, and individuals), technology issues or trends, future projections, case studies, or global characterizations.

(4) Timeliness for strategic reporting is an important consideration because it must be relevant to operational needs and other consumer requirements. Although it is not possible to designate a specific time requirement, once a consumer deadline has been established, the intelligence production element must meet that requirement on a timely basis.

(5) SIRs may be generated by any CND intelligence provider.

(6) Formatting for SIRs is flexible. However, SIRs will generally conform to DoD-wide standards such as the Intelligence Community Assessment.

4. Product Dissemination

a. The Services/Combatant Commands are required to use the primary reporting vehicle (i.e., JIMS). Analysis of network activity will be entered into the JIMS and thus available for the communities use as soon as feasible. Significant cyber events[11] should also be disseminated via message traffic to assure that immediate defensive/mitigation actions can be taken.

b. When organizational processes allow, all NIRs and strategic-level reports will be disseminated via automated message handling system (AMHS)/M3. It is up to the discretion of each organization to provide other means of dissemination such as posting to a Web page or via e-mail.

c. The message format should follow guidelines as stated above or as disseminated by USCYBERCOM.

5. Writing for Release

a. All classified reports will be written for the widest dissemination possible. If appropriate, one report may have multiple versions at different

[11] Cyber events are considered significant if they (1) occur more than one percent of the yearly incident total; (2) affect more than one DoD enclave; and (3) fall under incident handling categories 1, 2, 4, and 7.

classification levels (e.g., //REL TO USA, NATO or //REL TO FVEY (i.e., Australia, Canada, New Zealand, United Kingdom, and United States)).

b. All reports will include a "tear-line" or appendix for information, usually technical in nature, which is UNCLASSIFIED//FOR OFFICIAL USE ONLY. Inclusion of such an appendix will reduce ambiguity and provide clarity for the CND community on what information can be used in sensors.

6. USCYBERCOM "Smart Book". USCYBERCOM will manage a community "Smart Book." This book contains background information for the CND IC. Additional information, such as the standard format for Analyst Notebook Charts and organizational missions, will be maintained in this book. Currently, the "Smart Book" can be located on USCYBERCOM's JWICS Web page.

ENCLOSURE G

COMPUTER NETWORK DEFENSE INCIDENT HANDLING TOOLS

This enclosure provides an overview of common tools used by the computer network defense (CND) community to facilitate incident handling.

1. Joint Incident Management System (JIMS)

a. The JIMS is the central repository for managing all reportable events and incidents in the Department of Defense. It serves as the primary reporting mechanism for submitting reportable events and incidents to USCYBERCOM and is the basis for USCYBERCOM support to Combatant Commanders, senior government leaders, and civilian authorities.

b. The consistent, complete, and timely reporting of incident data into a single repository is necessary to reflect the collective reporting of adversarial activity. It can also help shape tactical, strategic, and military response strategies, providing local, intermediate, and DoD side situational awareness of CND activities, operations, and their impacts.

c. The CC/S/A/FAs provide reportable event and incident reports to the JIMS in the form of database records. These reportable event and incident records are integrated, correlated, and displayed using a variety of visualization applications, the combination of which provide the CND community with a shared situational awareness capability.

(1) Lessons Learned. CC/S/A/FAs are required to follow the policy and guidance provided in the Joint Lessons Learned Program (JLLP), CJCSI 3150.25D. The JLLP will contribute to joint capabilities integration, development, and improvement. The JLLP will enhance the joint operator's ability to learn from the conduct of operations across all levels of engagement and improve mission effectiveness.

(2) The Joint Lessons Learned Information System (JLLIS) is the System of Record for the JLLP and provides a Web-enabled information management system to meet operational needs for reporting lessons learned.

d. All organizations participating in the JLLP are to coordinate activities and collaboratively exchange observations, findings, and recommendations to the maximum extent possible.

e. CND Analysts use the Enterprise Sensor Grid (ESG) for collecting, processing, and storing the DoD networking sensing environment information (e.g., raw, processed, correlated, alert, etc.), facilitating execution of selected COAs to mitigate and respond to attacks directed at DoD information networks.

f. USCYBERCOM is the functional owner of the JIMS and maintains and manages it. Access to JIMS can be obtained through USCYBERCOM on SIPRNET.

2. Joint Malware Catalog (JMC)[12]

a. The JMC is the central repository for storing malware and associated analysis. It serves as the primary reporting mechanism for submitting software artifacts suspected of being adversarial tradecraft (e.g., viruses, rootkits, and worms).

b. The JMC is the basis for the Department of Defense's capability to rapidly analyze malicious code and provide an accurate understanding of its behavior and capabilities. By maintaining a current malware repository, the Department of Defense can leverage previous analytical experience, identify and respond to new attack techniques, and perform applied research to improve analysis capabilities.

c. The CC/S/A/FAs submit malware to the JMC. Malware recorded in the JMC can then be analyzed, viewed, correlated, and shared with other DoD organizations. Some analytical results are produced automatically using automated run-time analysis tools. More in-depth analysis may be conducted by technical analysts and recorded in the JMC to share with others.

d. The USCYBERCOM is the functional owner of the JMC. The USCYBERCOM maintains and manages the JMC. Access to the JMC can be obtained through USCYBERCOM.

3. CND Intelligence Analysis Tools

a. The primary CND intelligence analysis tool suite used to derive CND intelligence information is JIMS.

b. The JIMS analysis environment is available on the SIPRNET network and is intended to fuse intelligence with network incident reports to help shape response strategies and perform trending analysis and correlations.

c. JIMS data is comprised of all of the significant foreign-initiated computer intrusion or probe activity noted by incident analysts.

[12] The Joint MALWARE Catalog is currently under development. CND developers interested in participating should contact USCYBERCOM.

d. Intelligence analysts research the TTPs used by the adversary during each incident to ascertain what adversary may be responsible and if there is any additional associated suspicious activity with this or other DoD hosts.

e. Both classified and open source research are used in the analysis, and any derived intelligence is included in the JIMS.

f. The information and accompanying intelligence is provided in order to document this activity, and to help determine common methodologies and trends used by threat actors.

4. DoD Protected Traffic List

a. USCYBERCOM maintains the DoD Protected Traffic List at the following URL: http://www.cybercom.smil.mil. This list ensures critical DoD ISs are not affected inadvertently by responses to CND events.

b. This list includes Internet-NIPRNET traffic, enclave traffic, and key allied interoperability traffic. This technical data list includes IP addresses and TCP/IP ports, as well as operational impacts if protected traffic is blocked.

c. CC/S/A/FAs notify USCYBERCOM of any actions taken that affect the DoD Protected Traffic List. ISs on the DoD Protected Traffic List may be affected under extreme circumstances; therefore, it is imperative to identify the operational impact of actions taken prior to blocking traffic that may be on the protected traffic list.

5. DoD Enterprise Incident Sets

a. Incident sets are groups of related incidents and associated data requiring centralized management at the DoD level.

b. Incident sets may span multiple CC/S/A/FAs or merit DoD-level attention based on the scope or implications of the incidents.

c. Due to the strategic concern and implications of incident sets, USCYBERCOM notifies STRATJIC IO Division of incidents and actions taken.

d. The USCYBERCOM is the central manager for all DoD Enterprise Incident Sets. Incident sets are identified to the network operations community using CTOs, which designate:

(1) Incident set unique name.

(2) Summary description.

(3) POC information.

(4) Incident set signature indicators.

(5) Response action guidance for incidents meeting incident set criteria.

(6) Special reporting guidance for both technical reporting and operational reporting.

e. Tier II entities develop capabilities to track ongoing incident sets and determines if detected intrusions match criteria for inclusion.

f. Intrusions and/or alert data matching a defined incident set signatures are reported immediately to the USCYBERCOM.

g. Coordination and deconfliction activities with the LE/CI community for USCYBERCOM managed incident sets occur via the LE/CI organizations (at USCYBERCOM).

6. DoD Information Network Deception Projects

a. DoD entities deploying network deception programs (e.g., honey pots) report the device and/or program to the USCYBERCOM for situational awareness prior to connection to any DoD information network.

b. This information is used to deconflict sensor reports of suspicious activities or potentially vulnerable ISs.

c. Trusted agents within the USCYBERCOM safeguard system information. Information on deception projects include:

(1) Mission, intent, and purpose of the project.

(2) Location (Internet address(es) and types of device(s) (must include the WAN routable IP addresses).

(3) Type of data to be collected.

(4) POC for the device(s), to include telephone, e-mail, and organization.

7. Cyber Condition (CYBERCON)

a. The CYBERCON system is a uniform system of five progressive readiness conditions (CYBERCON 5, the least restrictive, through CYBERCON 1, the most restrictive) with options for offensive and defensive cyberspace operations, to include CND, Computer Network Exploitation (CNE), Computer Network Attack Operational Preparation of the Environment (CNA-OPE), CND-RAs, and CNA as authorized by DoD regulations. CYBERCONs describe graduated levels of readiness and response options that posture DoD components to secure, operate, and defend the DoD Information Network and to deter or defeat adversaries.

b. Commanders may raise CYBERCON levels to re-establish the confidence level of systems based on the tradeoff in resources. Alternatively, they may execute tailored readiness options to respond to specific intrusions or threats.

c. As component heads or commanders increase their CYBERCON level or implement Tailored Readiness Options (TROs), they will adjust their network footprint and configuration to ensure the availability and control of mission critical resources, and when authorized, conduct or request a CND-RA within the defined bounds of the action under DoD authority.

d. Operations in support of CYBERCON implementation will be executed in accordance with CJCSI 3121.01B and any approved supplemental authorities. CDRUSSTRATCOM's authority to set CYBERCON levels is derived from DoDD O-8530.1 and CJCSI 6510.01, and is consistent with UCP authorities to direct the operations and defense of the DoD Information Network.

(INTENTIONALLY BLANK)

ENCLOSURE H

REFERENCES

a. Federal Information Security Management Act, Title III, Information Security

b. OMB Circular No. A-130, “Management of Federal Information Resources”

c. DoDI O-8530.2, 9 March 2001, “Support to Computer Network Defense (CND)”

d. CJCSI 6510.01 Series, “Information Assurance (IA) and Support to Computer Network Defense (CND)”

e. Unified Command Plan (UCP), 6 April 2011

f. DoDI O-3600.02, 28 November 2005, “Information Operation (IO) Security Classification Guidance”

g. DoDI 5505.3, 21 June 2002, “Initiation of Investigation by Military Criminal Investigative Organizations”

h. CJCSI 3121.01 Series, “Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces”

i. CJCSM 3150.03 Series, “Joint Reporting Structure Event and Incident Reports”

j. DoD 5400.11-R, 14 May 2007, “Department of Defense Privacy Program”

k. Privacy Act of 1974, 5 U.S.C. 552a

l. OMB memorandum M-07-16, 22 May 2007, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”

m. OMB memorandum M-06-16, 23 June 2006, “Protection of Sensitive Agency Information”

n. OMB memorandum M-06-19, 12 July 2006, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.”

o. NIST Special Publication 800-86, August 2006, “Guide to Integrating Forensic Techniques into Incident Response”

p. “Investigations Involving the Internet and Computer Networks,” NCJ 210798. National Institute of Justice. Department of Justice (DOJ). January 2007. Web. 17 July 2009. http://www.ojp.usdoj.gov/nij/pubs-sum/210798.htm.

q. 18 U.S.C. 2510 et seq.

r. 18 U.S.C. 31212 et seq.

s. 18 U.S.C. 2701 et seq.

t. Federal Rules of Evidence Exception (803(6))

u. “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,” July 2002, Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice. Web: 15 July 2009, http://www.cybercrime.gov/s&smanual/

v. Electronic Communications Privacy Act (ECPA)

w. “Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition,” April 2008, National Institute of Justice, Department of Justice. Web: 17 July 2009, http://www.ojp.usdoj.gov/nij/pubs-sum/219941.htm

x. “Forensic Examination of Digital Evidence: A Guide for Law Enforcement,” April 2004, National Institute of Justice, Department of Justice. Web: 17 July 2009, http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm

y. “Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors,” January 2007, National Institute of Justice, Department of Justice. Web: 17 July 2009, http://www.ojp.usdoj.gov/nij/pubs-sum/211314.htm

z. CNSSI No. 1253, October 2009, “Security Categorization and Control Selection for National Security Systems”

aa. NIST SP 800-60, “Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories” bb. DoDI 8510.01, 28 November 2007, "DoD Information Assurance Certification and Accreditation Process (DIACAP)"

cc. NIST SP 800-61, March 2008, "Computer Security Incident Handling Guide"

dd. 18 U.S.C. 2511(2)(a)(i)

ee. CJCSI 3150.25D, "Joint Lessons Learned Program"

ff. Joint Publication 1-02 Series, "Department of Defense Dictionary of Military and Associated Terms"

gg. CNSSI No. 4009, "National Information Assurance (IA) Glossary"

hh. DoD O-8530.1-M, 17 December 2003, "Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process"

ii. DoDD 8100.1, 19 September 2002, "Global Information Grid (GIG) Overarching Policy"

jj. DoDD 8500.01E, 24 October 2002, "Information Assurance (IA)"

kk. "Joint Concept of Operations for Global Information Grid Network Operations"

ll. DoDI 8552.01, 23 October 2006, "Use of Mobile Code Technologies in DoD Information Systems"

mm. CJCSI 3150.25, "The Joint Lessons Learned Program"

nn. Joint Publication 5-0 Series, "Joint Operation Planning"

oo. CNDSP Evaluator's Scoring Metrics, "Certification and Accreditation", Ver. 8.0, 1 June 2011

pp. NIST SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations, Revision 3"

(INTENTIONALLY BLANK)

GLOSSARY

GLOSSARY PART I—ABBREVIATIONS AND ACRONYMS

ACL	access control list
AO	Authorizing Official
AOR	area of responsibility
ARP	address resolution protocol
AS&W	attack sensing and warning
AV	antivirus
B	
B/P/C/S	base/post/camp/station
BDA	battlefield damage assessment
C	
C2	command and control
CAT	category
CCC	C4 Control Center
CC/S/A/FA	Combatant Command/Service/Agency/Field Activity
CCIR	Commander's Critical Information Requirement
CERT	computer emergency readiness team
CI	counterintelligence
CIO	chief information officer
CIRT	computer incident response team
CND	Computer Network Defense
CNDRA	Computer Network Defense Response Actions
CNDSP	Computer Network Defense Service Provider
COA	course of action
CTO	communications tasking order
CUI	Controlled Unclassified Information
CYBERCON	cyber condition
D	
DAA	Designated Accrediting Authority, now known as the Authorizing Official
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DLL	Dynamic-Link Library
DNC	DISA NetOps Center
DoD	Department of Defense
DoDI	Department of Defense instruction
DOJ	Department of Justice

DOS	Department of State
DoS	denial of service
DSN	Defense Switch Network
DTG	date-time group
E	
ECPA	Electronic Communications Privacy Act
ESG	Enterprise Sensor Grid
F	
FISMA	Federal Information Security Management Act
FRAGORD	fragmentary order
G	
GNCC	Global Network Operations Control Center
GNSC	Global Network Support Center
H	
HQ	headquarters
I	
I&W	indications and warning
IA	information assurance
IAPC	Information Assurance Protection Center
IAVM	information assurance vulnerability management
IAW	in accordance with
IC	Intelligence Community
ICCWG	International CND Coordination Working Group
IC-IRC	Intelligence Community–Incident Response Center
IDS	intrusion detection system
IIMG	Interagency Incident Management Group
IM	instant messaging
IO	information operations
IP	Internet Protocol
IPS	intrusion prevention system
IS	information system
ISAC	Information Sharing and Analysis Center
ISP	Internet service provider
IT	information technology
J	
JEL	Joint Electronic Library
JIMS	Joint Incident Management System
JMC	Joint Malware Catalog
JLLIS	Joint Lessons Learned Information System

JLLP	Joint Lessons Learned Program
JTIP	Joint Threat Intelligence Portal
JWICS	Joint Worldwide Intelligence Communications System
L	
LAN	local area network
LE	law enforcement
LE/CI	law enforcement and counterintelligence
LES	law enforcement sensitive
M	
MAC	mission assurance category
MB	megabyte
N	
NAI	named area of interest
NCRCG	National Cyber Response Coordination Group
NIPRNET	Non-Secure Internet Protocol Router Network
NIR	Network Intelligence Report
NIST	National Institute of Standards and Technology
NGA	National Geospatial-Intelligence Agency
NOSC	Network Operations Security Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	Network Service Centers
NTOC	National Security Agency/Central Security Service Threat Operations Center
O	
OI	operational impact
OMB	Office of Management and Budget
OPORD	operation order
OPREP	operational report
OPSEC	operations security
OS	operating system
OSD	Office of the Secretary of Defense
P	
P2P	peer-to-peer
PII	personally identifiable information
POC	point of contact
R	
RA	Response Actions
RAM	random-access memory

S	
SA	situational awareness
SCI	sensitive compartmented information
SIPRNET	Secret Internet Protocol Router Network
SIR	Strategic Intelligence Report
SJA	Staff Judge Advocate
STIG	Security Technical Implementation Guides
STRATJIC	USSTRATCOM Joint Intelligence Center
T	
TASKORD	tasking order
TCCC	Theater C4I Control Center
TCP	Transmission Control Protocol
TDY	temporary duty
TI	technical impact
TID	Threat Identification Database
TNC	Theater NetOps Center
TNCC	Theater Network Control Center
TPFDD	time-phased force deployment data
TRO	tailored readiness option
TS	Top Secret
TTP	tactics, techniques, and procedures
U	
URL	Uniform Resource Locator
USB	universal serial bus
US-CERT	United States–Computer Emergency Readiness Team
USCYBERCOM	U.S. Cyber Command
USSTRATCOM	U.S. Strategic Command
W	
WAN	wide area network
WARNORD	warning order

GLOSSARY PART II—DEFINITIONS

Unless otherwise stated, the terms and definitions contained in this glossary are for the purposes of this manual only. Unless indicated by a parenthetic phrase after the definition that indicates the source publication or document, these terms have not been standardized for general, DoD-wide use and inclusion in the Department of Defense Dictionary of Military and Associated Terms (JP 1-02) (reference ff). In some cases, JP 1-02 may have a general, DoD-wide definition for a term used here with a specialized definition for this instruction.

<u>accreditation decision</u>. See CNSSI No. 4009, “National Information Assurance (IA) Glossary” (reference gg).

<u>attack sensing and warning (AS&W)</u>. See CNSSI No. 4009 (reference gg).

<u>availability</u>. See CNSSI No. 4009 (reference gg).

<u>blue team</u>. See CNSSI No. 4009 (reference gg).

<u>command authority</u>. See CNSSI No. 4009 (reference gg).

<u>Commander’s Critical Information Requirement (CCIR)</u>. An information requirement identified by the commander as being critical to facilitating timely decision making.

<u>component CND authority</u>. See reference hh.

<u>computer network defense (CND)</u>. Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.

<u>computer network defense (CND) operational hierarchy</u>. See reference hh.

<u>computer network defense response actions (CND RAs)</u>. CJCSI 3121.01 Series, “Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces”

<u>computer network defense (CND) services</u>. See reference hh.

<u>computer network defense service provider (CNDSP)</u>. See reference hh.

confidentiality. See CNSSI No. 4009 (reference gg).

counterintelligence. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

counterintelligence activities. The four functions of counterintelligence are operations; investigations; collection and reporting; and analysis, production, and dissemination.

counterintelligence investigation. An official, systematic search for facts to determine whether a person is engaged in activities that may be injurious to U.S. national security or advantageous to a foreign power.

cyber incident. Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

enclave. See CNSSI No. 4009 (reference gg).

enterprise CND sensor grid. A coordinated constellation of independently owned and implemented intrusion and anomaly detection systems deployed throughout DoD information systems and computer networks. The CND sensor grid supports sensing capabilities for NetOps.

event. Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. See CNSSI No. 4009 (reference gg).

fragmentary order. An abbreviated form of an operation order issued as needed after an operation order to change or modify that order or to execute a branch or sequel to that order (reference ff).

General Service Network or System (GENSER). See reference hh.

Global Information Grid. See CNSSI No. 4009 (reference gg).

incident handling. The detection, analysis, and response to any cyber event or incident for the purpose of mitigating any adverse operational or technical impact.

indications and warning (I&W). See reference hh.

information assurance (IA). Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein (reference gg).

information assurance vulnerability management (IAVM). The comprehensive distribution process for notifying CC/S/A/FAs about vulnerability alerts, bulletins, technical advisories, and countermeasures information. The IAVM program requires CC/S/A/FA receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability.

Information Sharing and Analysis Center (ISAC). Mission is to advance the physical and cyber security of the critical infrastructures by establishing and maintaining a framework for valuable interaction between and among ISACs and with government (http://www.isaccouncil.org).

integrity. See CNSSI No. 4009 (reference gg).

Joint Malware Catalog. The Joint Malware Catalog is the central DoD repository for storing malware and associated analysis. It serves as the primary reporting mechanism for submitting software artifacts suspected of being adversarial tradecraft (e.g., viruses, rootkits, and worms).

Joint Incident Management System (JIMS). JIMS is the central catalog for managing event and incident reports. The primary objective of JIMS is to ensure the timely flow of crucial network intelligence across DoD/USG and ally boundaries; to reflect the collective reporting of adversarial activity; to assist in shaping tactical, strategic, and military response strategies; and to perform trending analysis, correlation, and fusion.

Joint Lessons Learned Program (JLLP). Establishes policy, guidance and responsibilities for the CJCS Joint Lessons Learned Program (JLLP) and codifies the Joint Lessons Learned Information System (JLLIS) as the DoD system of record for the JLLP.

Mission Assurance Category. See reference jj.

network operations (NetOps). NetOps is defined as the operational construct consisting of the essential tasks (DoD Information Networks Network Defense, DoD Information Networks Enterprise Services, and content staging/ information dissemination management), situational awareness (SA), and C2 that USSTRATCOM will use to operate and defend DoD Information Networks. The three desired effects of NetOps are assured system and network availability, assured information protection, and assured information delivery (reference kk).

operation order (OPORD). A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation (reference ff).

red team. See CNSSI No. 4009 (reference gg).

reportable event. An event that may, or may not, result in an incident, but is required to be reported in accordance with this manual or other DoD reporting guidelines (e.g., OPREP 3 reporting).

special enclave. DoD information systems and/or computer networks with special security requirements (e.g., special access programs, special access requirements).

system. See CNSSI No. 4009 (reference gg).

tasking order (TASKORD). A method used to task and to disseminate to components, subordinate units, and command and control agencies projected targets and specific missions (reference ff).

trusted media. Media provided by a trusted source that is adjudged to provide reliable software code and/or information and whose identity can be verified by authentication**.**

trusted source. A software and/or information source that is adjudged to provide reliable software code and/or information and whose identity can be verified by authentication (reference ll).

trusted toolkit. Tools provided by a trusted source that are adjudged to provide reliable software code and/or information and whose identity can be verified by authentication**.**

vulnerability assessment. See CNSSI No. 4009 (reference gg).

warning order (WARNORD). A WARNORD is a planning directive that initiates the development and evaluation of military COAs by a supported commander and requests that the supported commander submit a commander's estimate (reference ff).