Fantastic Incident Response Plan (IRP)

DISTRIBUTION STATEMENT D: Distribution authorized to DOD and United States (U.S.) DOD contractors only; Internal Documents; July 2020.
DESTRUCTION NOTICE: Non-record FOUO documents may be destroyed by shredding or tearing into pieces, and discarding pieces in regular trash containers.

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Introduction

A Cyber Incident is defined as, “An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies with increased attack frequency in recent years on United States Government owned Information Systems (ISs) and networks, it is imperative that Organization implement a well-defined Incident Response (IR) capability. Organization faces challenges of protecting both classified and Controlled Unclassified Information (CUI) on IS. Protection, identification, containment, eradication, and recovery for security incidents require technical knowledge, communication, and coordination among those responsible for protecting Organization resources. Depending upon level and complexity of an incident, it could take days, weeks, or even months to reestablish system integrity when Organization infrastructure has been compromised.

This Incident Response Plan (IRP) is developed in accordance with guidelines and procedures provided in References (a) through (h). References (i) through (qq) provide supplementary guidance on cyber system, information, and personnel security. This plan provides information and guidance to process IS disruptions and security incidents within Organization. IS disruptions are included as they are often first sign of an incident.

1.2 Purpose

Organization IRP documents procedures to coordinate identification of system disruptions, security incidents, and reporting process.

Organization IRP is predicated on:

- Protecting information and ISs
- Reporting incidents
- Detecting attacks or intrusions
- Mitigating effects of incidents
- Restoring services
- Reporting and documenting lessons learned

1.4 Applicability and Scope

This IRP describes four stages of incident handling in Figure 1, as defined in CJCSM 6510.01B. Figure 1 focuses on preparation and post-incident activities and includes reporting guidelines and requirements. This document satisfies cybersecurity (CS) requirements for confidentiality, integrity and availability of systems and data, and provides technical, administrative, personnel, physical, and procedural implementations for network components within Organization.

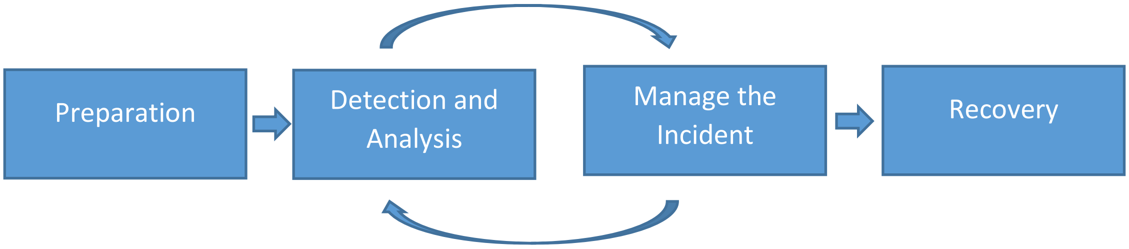

Figure 1. National Institute of Standards and Technology (NIST) IR Phases

Preparation

•Have a plan in place

•Know how to use the plan for events & incidents

Detection & Analysis

•Identify an incident occurrence

•Take appropriate action

Containment, Eradication & Recovery

•Contain the scope and magnitude of the incident

•Remove the cause of the incident

•Restore system to normal operations

Post-Incident Activity

•Most critical step often overlooked

•Lessons learned, prosecution (if necessary), policy or SOP revision

1.5 Reporting Structure

The incident reporting community is organized into levels: Command, Center, and Local. For purposes of this plan, incidents, and reportable events, as defined in Section 4.0, will be reported to appropriate points of contact (POC). Organization personnel shall not bypass Organization reporting structure by reporting directly to a higher authority.

2.0 ROLES AND RESPONSIBILITIES

A critical facet of incident response is preparation before an incident. Without adequate preparation, response efforts will likely be disorganized and confused. Preparation limits damage potential by ensuring responsible actions are known and coordinated. Planning is an integral part of security policy.

Users are responsible for reporting suspected intrusions to appropriate points of contact. This document outlines critical incident handling roles and responsibilities for user, local Command Information Systems Security Manager (ISSM), Cyber Incident Response Team Leader, and Incident Response Team (IRT) and supporting functions. Each role, with exception of users, is responsible for creating and maintaining Standard Operating Procedures (SOPs) applicable to this IRP.

2.1 Commanding Officer (CO)

Commanding Officer (CO) is ultimately responsible for implementing the CS program including workforce training and certification. CO will appoint a Command ISSM and Command Security Manager.

2.2 Command Security Manager (CSM)

Command Security Manager (CSM) is responsible to the CO for proper command personnel security posture development, implementation and enforcement. CSM will work with the command ISSM to develop the appropriate physical security posture of command information systems. CSM is also responsible for security clearance information, physical evidence handling, and liaison with Naval Criminal Investigative Service (NCIS). Also, responsible for reporting criminal intrusions or incidents to NCIS and coordinating ensuing investigation.

2.3 Public Affairs Office (PAO)

PAO coordinates and disseminates internal and external communication products, media relations, and community outreach processes, procedures and reporting requirements. PAO responds to information requests from customers and federal, state, and local government agencies and ensures responses conform to official guidance. Prepares incident related news releases, feature stories, speeches, blog posts, and articles.

2.4 Organization Cybersecurity Program Manager

The Organization Cybersecurity Program Manager ensures the command's IH program is managed in accordance with Navy guidance (Reference (g)) by overseeing incident reporting from initial reports through closeout; triage; eradication and corrective action, and process improvement.

2.5 Command Information Systems Security Manager (CISSM)

Command Information Systems Security Manager (CISSM) is responsible for ensuring that command's information systems are operated, used, and maintained in compliance with prescribed security policies and practices. ISSM is focal point for organizational IS security concerns.
CISSM is responsible for:

- Ensuring evidence is properly obtained, marked, and protected.
- Ensuring Information Systems Security Officer (ISSO) or Incident Response Team (IRT) initiate, complete, and retain appropriate Incident Response (IR) worksheets and checklists in accordance with records retention policy.
- Providing incident information to IRT and appropriate service and agency organizations within prescribed timelines.
- Advising CO after identifying a serious security incident and coordinating response with CSM.
- Implementing overall IS Security Program (ISSP) ensuring that IS security related incidents and violations are immediately reported, properly investigated, and correctly resolved.
- Coordinating targeted monitoring activities, to include appropriate notification to Judge Advocate General (JAG), Organization CSM, and CO for monitored systems.

methodologies to assist investigating personnel in resolving problems.

- Collecting local Command component audit records and reviewing and retaining local security audit trail.
- Maintaining a notification list for Organization command personnel, Cyber Security Defense and Operations (CSDO), and Naval Network Warfare Command (NNWC).
- Formally designating IRT members and ensuring they are properly trained for their duties.
- Ensuring that Organization IH Jump bag is functional and current.

2.6 Incident Response Team (IRT)

Organization CISSM appoints an IRT that is responsible for IS security during an event or incident. Team consists of CISSM as Team Leader/Historian, a data extraction specialist or system-scanning specialist, DCC, and CSM. Additional team members are assigned as necessary.

Depending on incident severity, local IRT may be augmented by Navy Information Operations Command (NIOC) or Navy Cyber Defense Operations Command (CSDO) personnel. Organization IRT is the first level of interaction with Navy Help Desk and CSDO after logging users experiencing security incidents.

Organization IRT's responsibilities include:

- Ensuring appropriate team members are approved Privileged Users and have completed training for their position including evidence collection and processing.
- Coordinating incoming information, advising users on handling low-level security incidents, passing information through the chain of command, and disseminating information to the appropriate audience. Reporting security incidents or security practice deviation in accordance with Organization policies and procedures.
- Notifying appropriate personnel and agencies (e.g., Navy Help Desk, Intranet, CSDO or Big Command (BComm)) of security incidents and requesting assistance when necessary.
- Reviewing and analyzing security-related events and security violations or failures
- With appropriate technical assistance, investigating security violations to determine cause and appropriate actions to prevent recurrence
- Generating incident reports for each security incident.

2.8 Intranet Help Desk

Responsible for:

- Providing immediate support to local Command ISSM and IRT during identification, containment, investigation, and post-incident activity.
- Logging security incidents into helpdesk system.
- Assigning incident tickets.
- Notifying local Command ISSM and ACTR in accordance with IT Help Desk procedures.
- Responsible for reporting suspicious events or incidents to appropriate Computer Network Defense Service Provider (CSSP-CSDO)

2.9 Organization Users

Despite advances in automated intrusion detection systems, users may discover many intrusions and cyber incidents effectively. Users must be vigilant for unusual system behavior that indicate a security incident is in progress.

Organization Users are responsible for:

- Are required to complete DOD cyber awareness training annually as required by CJCSM 6510.01B. Organization strives for a sustained, professional CS workforce with knowledge and skills to effectively prevent and respond to attacks against government information, information systems, and infrastructure. Immediately reporting suspected security violations, to include compromise, component failure, abnormal system behavior, and vulnerabilities to the appropriate authorities.
- Complying with Organization security policies and procedures.
- Preserving evidence.
- Cooperating with investigative personnel

2.10 System Owner

Depending on the incident, System Owners may coordinate with Command ISSM and IRT to take action during an incident investigation.

3. 0 EVENTS/INCIDENTS

Defining events and incidents are challenging IR process aspects. This section provides explanations, common types, and differentiation between events and incidents.

3.1 Event

An event is an occurrence not yet assessed that may affect performance of an IS or network. Events include unplanned system reboots, system crashes, packet flooding, or a core service outage affecting availability of a system or network and may indicate an incident is in progress.

3.2 Incident

An incident is an assessed occurrence with potential or actual adverse effects to an IS. A security incident is an event or series of events that violate security policy. Security incidents include unauthorized parties penetrating a computer system, exploiting technical or administrative vulnerabilities, or introducing computer viruses or malicious code. Examples are unauthorized use of another user's account or system privileges or executing malicious code.

3.3 Security Incident Handling (IH)

A Security IH process outlines detailed reporting steps and remedial actions to protect ISs affected by security incidents. Incident handling includes forming a team with adequate technical capabilities, contacting appropriate resources, and closeout reporting after an incident is resolved.

3.4 Technical Vulnerability

A technical vulnerability is a hardware, firmware, or software weakness or design deficiency that leaves a system open to potential exploitation, either internally or externally, that increases risk of compromise, alteration of information, or denial of service.

3.5 Administrative Vulnerability

An administrative vulnerability is a security weakness caused by incorrect or inadequate security feature implementation created by a user, security, or system administrator action or inaction.

3.6 Types of Incidents

There are at least four general causes of computer security incidents:

- **Malicious Code.** Malicious code is software or firmware intentionally inserted into an IS for an unauthorized purpose.

- **System and Procedure Failures or Improper Acts.** A secure operating environment depends upon proper operation and use. Failure to comply with established procedures, or errors and limitations in procedures or system, can damage or increase vulnerability and risk. While advances in computer technology enable more security in ISs, much depends on those who operate and use information systems. Improper acts may be differentiated from an insider attack according to intent. Improper acts are committed when policy and procedure violations are intentional even if there is no evidence of system damage or information compromise.

  - Spills <COME BACK>

- **Intrusions or Break-Ins.** An unauthorized individual intrudes or gains access into a system.

- **Insider Attack.** Insider attacks provide the greatest risk. A trusted user or operator attempts to damage system or compromise information. As part of the onboarding process and annually thereafter (at a minimum), all Organization users complete insider threat training. The training coupled with this document identifies some of the potential risk indicators (PRI) associated with insider threat, such as ignorance, complacency, and malice. Some examples include, unknowingly clicking on a phishing scam, using personal storage devices (e.g., phone) for conducting official business without authorization, and attempting to access information or physical spaces that are not relevant to a work assignment. In the event one or more PRIs are observed, the PRI(s) must be reported to the Organization ISSM immediately. The Organization ISSM shall coordinate the investigation for all reports of potential insider threat following internal procedures.

The term "*incident*" encompasses general categories of adverse events:

- **Data Destruction or Corruption.** Data integrity loss can take many forms including file permission changes to enable non-privileged user access, malicious data or program file deletion, audit file changes to obscure an intrusion, unauthorized configuration file changes, or corrupt information imported from other sources.

- **Data Compromise.** Data compromise is information exposed to an unauthorized individual through either clearance level or inappropriate access authorization.

- **Malicious Code.** Malicious code attacks include viruses, Trojan Horse programs, worms, or scripts used by attackers to gain privileges, capture passwords, or modify audit logs to hide unauthorized activity. Malicious code is particularly troublesome as it is typically written to obscure its presence and is often difficult to detect. Malicious code, such as viruses and worms, replicate rapidly making containment difficult. It is usually propagated by a triggering mechanism, such as a particular time or event, intended to delete or corrupt files, or send data. A self-replicating malicious program segment may be stand-alone or attach to an executable system component attempting to leave no obvious evidence of its presence.

- **Privileged User Misuse.** Privileged user misuse occurs when a trusted user or operator attempts to damage a system or compromise information contained within.

- **Security Support Structure (SSS) Configuration Modification.** Software, hardware, and system configurations contributing to Security Support Structure (SSS) are controlled as essential system security policies. Unauthorized modification increases risk to a system.

- **Unauthorized access**. Unauthorized access to files and directories stored on a system or storage media through password theft, unauthorized privileges, network intrusion, and other malicious acts.

- **Unauthorized utilization of services**. Misusing available services.

- **Disruption of service**. Electronic mail (email) spamming, flooding a user account with email, or installing a malicious Trojan Horse program to alter system functionality.

- **Misuse.** Using Government Systems for other than official use.

- **Espionage**. Stealing information to subvert interests of government.

- **Hoaxes.** Spreading false information about incidents or vulnerabilities.

3.7 Avenues of Attack

Potential attack vectors include:

- Vulnerable local networks
- Unauthorized devices (including connections to a local network)
- Gateways to outside networks
- Communication devices, such as modems and wireless access points
- Shared electronic media
- Unapproved software downloaded from the Internet
- Direct physical access

3.8 Effects of an Attack

There are at least four effects of attacks that compromise computer security:

- **Denial of Service.** Any action to stop, interrupt, or degrade all or part of network service sufficiently to impact operations. Denial of service includes network flooding, introducing fraudulent packets, and system crashes or poor system performance where users are unable to effectively use computing resources.

- **Data or Programs Loss or Alteration.** Loss or alteration of data or programs would include an attacker who penetrates a system then modifies an operating system program or configuration file so that intrusion detection is unlikely.

- **Protected Data Compromise.** A major computer security incident hazard is information compromise or unauthorized classified information release that jeopardizes national security. Efficient incident handling minimizes this danger.

- **Loss of Trust in Computing Systems.** A computing system with high incident or event frequency degrades user trust as reliable to control confidentiality, integrity, and availability.

4.0 REPORTING GUIDELINES

Users noticing anomalous or suspicious activity (incident or reportable event) should report it immediately to Navy Help Desk, System ISSO, or Command ISSM, who will assess whether it is a local event or an event reportable to CSDO. Table 4-1 is a list of events and incident types to help identify incident types with operational significance. The list has examples of reportable incidents and event priorities for reporting information to local Command ISSM/IRT.

4.1 Incident Categories

An incident, or Reportable Event Category, is a collection of events or incidents sharing a common underlying cause useful for determining whether an incident or event is reportable.
Each event or incident is associated with one or more categories as part of incident handling process. Incidents reported to local Command ISSM/IRT shall be categorized according to framework outlined in Table 2.

Table 2: Incident Categories

Category	Description
0	**Exercise or Red Team Activity**
1	**Root Level Intrusion (Incident)** – Unauthorized privileged access to a DOD system. Privileged access, often referred to as administrative or root access, provides unrestricted access to system. This category includes unauthorized access to information or account credentials that could be used to perform administrative functions, e.g., domain administrator. If system 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 a DOD system. Non-privileged access, often referred to as user-level access, provides restricted access to system based on privileges granted to user. This includes unauthorized access to information or account credentials that could be used to perform user functions such as accessing Web applications, portals, or other similar information resources. If system 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 a DOD system that is defeated by normal defensive mechanisms. Attacker fails to gain access to DOD system, i.e., attacker attempt valid or potentially valid username and password combinations, and activity cannot be characterized as exploratory scanning. Reporting of these events are critical for gathering of useful effects-based metrics for Commanders.
4	**Denial of Service (Incident)** – Activity that denies, degrades or disrupts normal functionality of a system or network.
5	**Non-Compliance Activity (Event)** – Activity that potentially exposes DOD systems to increased risk as a result of 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 are critical for gathering of useful effects-based metrics for Commanders.
6	**Reconnaissance (Event)** – Activity that seeks to gather information used to characterize DOD systems, applications, networks, or users that may be useful in formulating an attack. This includes activity such as mapping DOD networks, system devices and applications, interconnectivity, and users or reporting structures. 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 purpose of gaining access to resources or information without consent or knowledge of user. This only includes malicious code that does not provide remote interactive control of compromised system. Malicious code that has allowed interactive access shall fall under incident Category 1 or 2, not 7. Interactive access may include automated tools that establish an open channel of communication to and/or from a DOD system.
8	**Investigating (Event)** – Events that are potentially malicious or anomalous activity deemed suspicious and warranted, or are undergoing further review. An event will not be closed out as a Category 8. A Category 8 event will be re-categorized to 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 criteria for other categories. This includes events such as system malfunctions or false alarms. When reporting these events, reason for which it cannot be otherwise categorized must be clearly specified.

4.2 Incident Precedence

In cases where more than one category applies, a category assigned is determined using the precedence indicated in Table 3.
For example, a reported incident could be either a User Level Intrusion (Category 2) or a Non-Compliance Activity (Category 5). User Level Intrusion takes precedence based on Table 3, and such incidents are reported as a User Level Intrusion (Category 2).

Table 3: Category Precedence

Precedence	Category	Description
0	0	Exercise or Red Team Activity
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)

4.3 Responding to an Incident

There are four stages of response.

4.3.1 Prepare (Pre-Incident Event)

This phase consists of the following items:
- Protect systems
- Document incident response, firewall, backup, & recovery procedures
- Acquire appropriate resources. Update IH jump bag
- Document and maintain incident response points of contact
- Establish and exercise training
- Perform an IR exercise annually as a minimum

4.3.2 Events Detection (Phase II)

This step identifies whether an incident has occurred and when IRT should take appropriate actions.
Typical actions:
- Investigate Events/Logs
- Acquire Full System Backup(s) or images
- Note Observations (e.g., Legal Requirements such as chain of custody, etc.)
- Notify authorized stakeholders (CO, ISSM, CSM, etc.)
- Consider INFOCON Change
- Determine if an incident occurred and identify type o Data Transfer Agent (DTA)

o Removable media (RM)

o Universal Serial Bus (USB) violations
o Denial of Service (DOS) attack

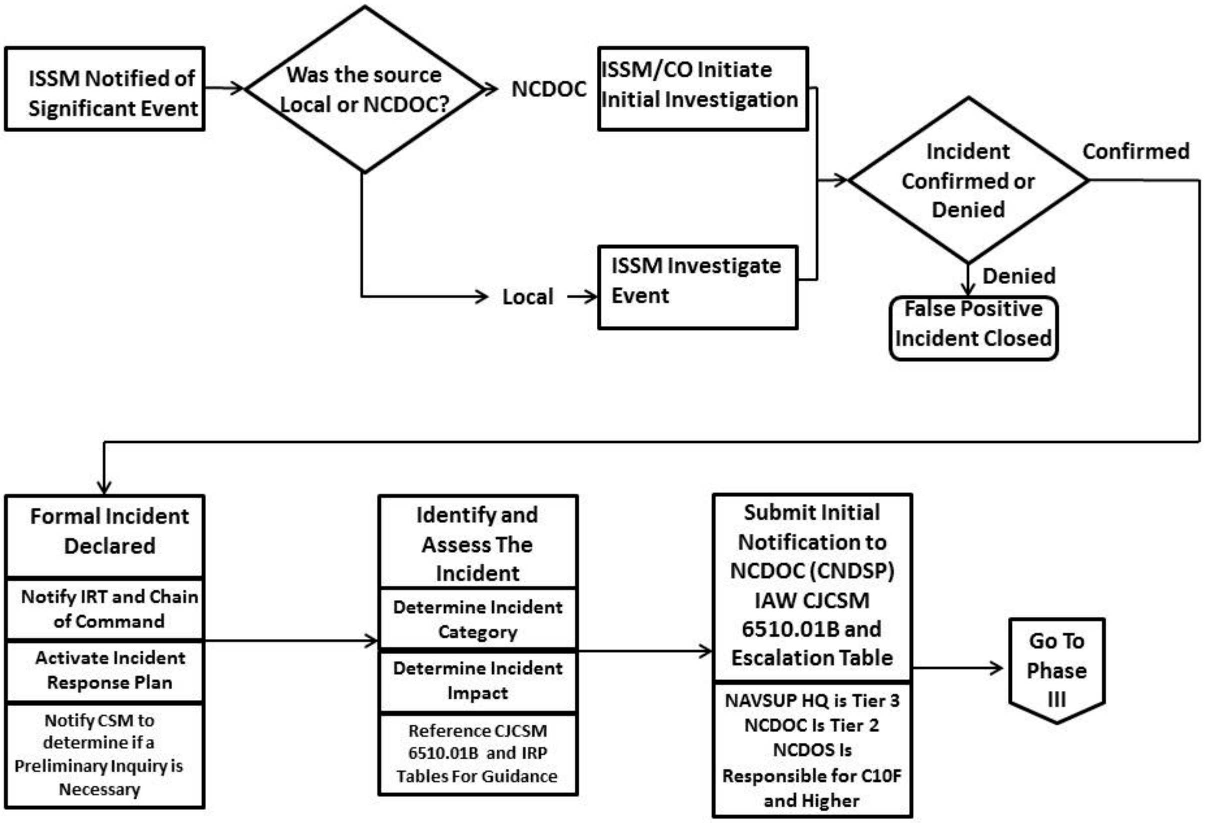
ISSM Notified of Significant Event
Was the source Local or NCDOC?
NCDOC
ISSM/CO Initiate Initial Investigation
Local
ISSM Investigate Event
Incident Confirmed or Denied
Confirmed
Denied
False Positive Incident Closed
Formal Incident Declared
Notify IRT and Chain of Command
Activate Incident Response Plan
Notify CSM to determine if a Preliminary Inquiry is Necessary
Identify and Assess The Incident
Determine Incident Category
Determine Incident Impact
Reference CJCSM 6510.01B and IRP Tables For Guidance
Submit Initial Notification to NCDOC (CNDSP) IAW CJCSM 6510.01B and Escalation Table
NAVSUP HQ is Tier 3
NCDOC Is Tier 2
NCDOS Is Responsible for C10F and Higher
Go To Phase III

Figure 3. Detection and Analysis (Phase II)

4.3.3 Containment, Eradication and Recovery (Phase III)

Containment limits incident scope and magnitude. Many incidents involve malicious code that can spread rapidly causing extensive damage and information loss. Once an incident is recognized, containment begins immediately. Steps include:

- Notify CSDO, Organization, and others as appropriate
- Limit scope of incident or event
- Change INFOCON
- Deploy IRT
- Preserve chain of custody
- Determine risk

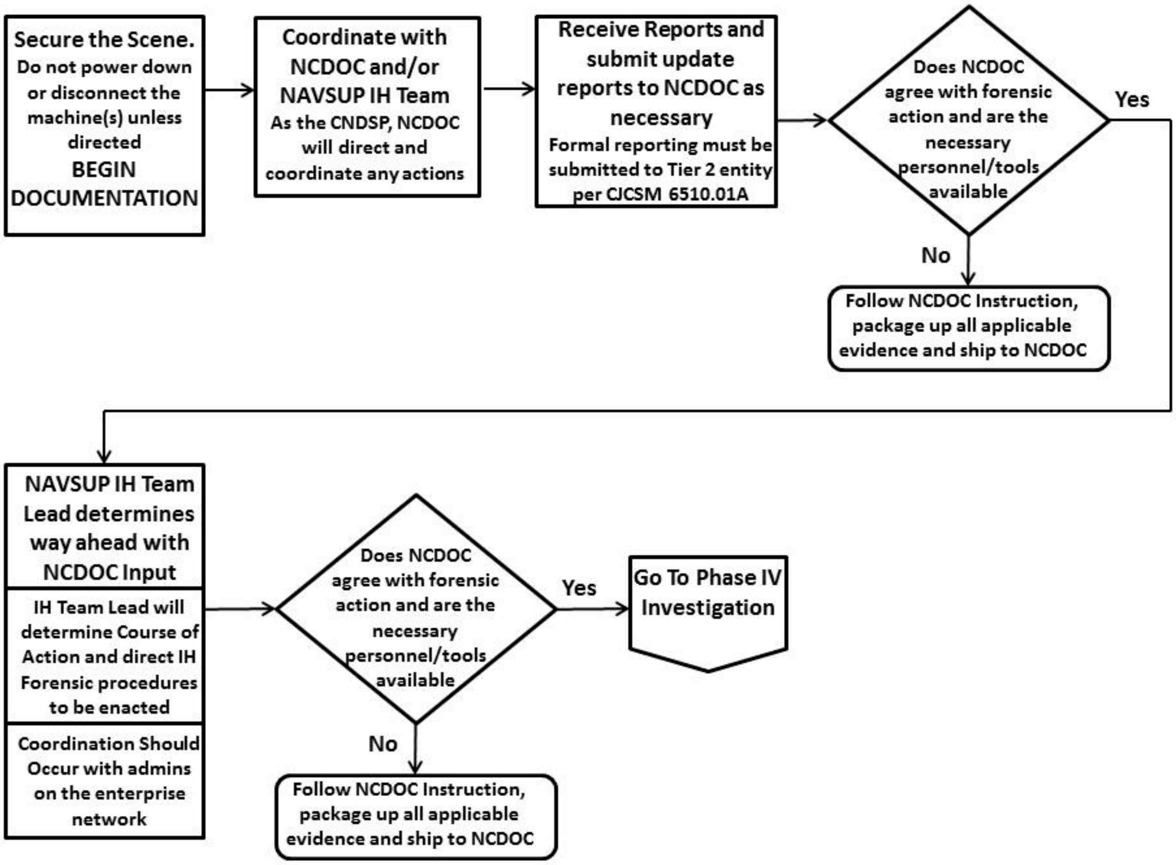
Secure the Scene.
Do not power down or disconnect the machine(s) unless directed
BEGIN DOCUMENTATION
Coordinate with NCDOC and/or NAVSUP IH Team
As the CNDSP, NCDOC will direct and coordinate any actions
Receive Reports and submit update reports to NCDOC as necessary
Formal reporting must be submitted to Tier 2 entity per CJCSM 6510.01A
Does NCDOC agree with forensic action and are the necessary personnel/tools available
Yes
No
Follow NCDOC Instruction, package up all applicable evidence and ship to NCDOC
NAVSUP IH Team Lead determines way ahead with NCDOC Input
IH Team Lead will determine Course of Action and direct IH Forensic procedures to be enacted
Coordination Should Occur with admins on the enterprise network
Does NCDOC agree with forensic action and are the necessary personnel/tools available
Yes
No
Go To Phase IV Investigation
Follow NCDOC Instruction, package up all applicable evidence and ship to NCDOC

Figure 4. Containment, Eradication and Recovery (Phase III)

Resolving incidents can be difficult and may involve virus removal, rebuilding systems, restoring backups, dismissing users, or perpetrator prosecution. Steps include:

- Identify root causes of incident
- Remove cause of event or incident
- Perform vulnerability analysis
- Implement protective techniques
- Consider legal action

Restoring a system to its normal business status is essential. Once complete, it is important to verify that restoration was successful and that system is back to normal condition. Steps include:

- Determine integrity of backup
- Restore operations
- Verify that restoration included hardened security configurations
- Monitor systems and network
- Consider INFOCON change to level established before the incident

4.3.4 Investigation and Post-Incident Activity (Phase IV)

Some incidents expend considerable resources. Once resolved, there is little interest in applying effort to post-incident activities. Follow-up procedures are a critical activity of incident response and supports efforts to prosecute those who have broken law. One example is modifying corporate policy to incorporate lessons learned during the incident handling process and countering vulnerabilities that allowed the incident to occur in the first place. Steps include:

- Analyze Incident
- Account for cost of incident
- Document event, report, and ensure evidence preservation
- Review Policies/Procedures for Lessons Learned
- Update Contingency Planning and Disaster Recovery procedures as needed.
- Implement Changes (if approved)

4.3.4.1. Contingency Planning (Phase IV)

- The process outlined in the Contingency Plan must be reviewed annually against the recorded incidents from the previous year.

- The Contingency Plan must be tested annually. Refer to section X of the Contingency Plan.

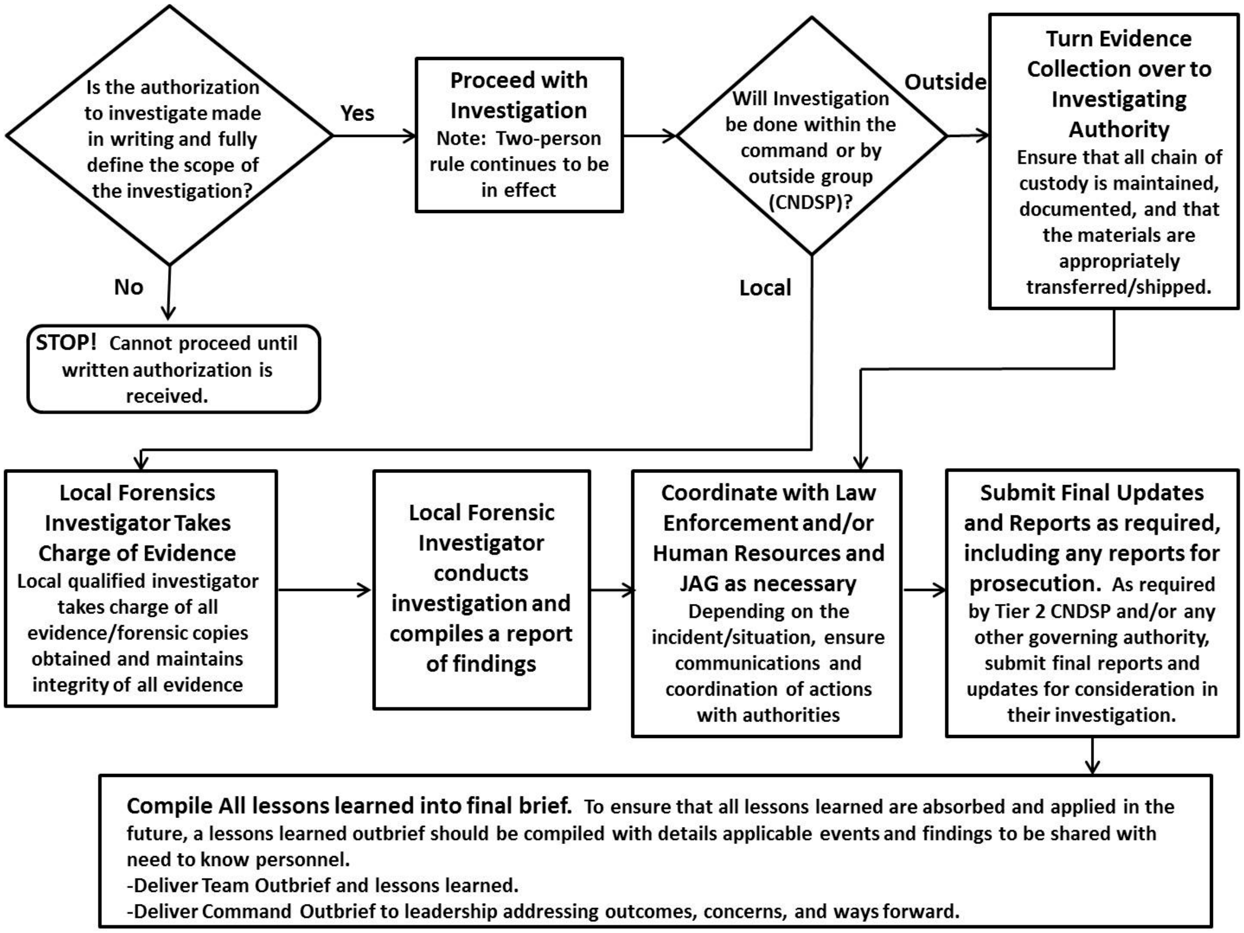
Is the authorization to investigate made in writing and fully define the scope of the investigation?
Yes
No
STOP! Cannot proceed until written authorization is received.
Proceed with Investigation Note: Two-person rule continues to be in effect
Will Investigation be done within the command or by outside group (CNDSP)?
Outside
Local
Turn Evidence Collection over to Investigating Authority Ensure that all chain of custody is maintained, documented, and that the materials are appropriately transferred/shipped.
Local Forensics Investigator Takes Charge of Evidence Local qualified investigator takes charge of all evidence/forensic copies obtained and maintains integrity of all evidence
Local Forensic Investigator conducts investigation and compiles a report of findings
Coordinate with Law Enforcement and/or Human Resources and JAG as necessary Depending on the incident/situation, ensure communications and coordination of actions with authorities
Submit Final Updates and Reports as required, including any reports for prosecution. As required by Tier 2 CNDSP and/or any other governing authority, submit final reports and updates for consideration in their investigation.
Compile All lessons learned into final brief. To ensure that all lessons learned are absorbed and applied in the future, a lessons learned outbrief should be compiled with details applicable events and findings to be shared with need to know personnel.
-Deliver Team Outbrief and lessons learned.
-Deliver Command Outbrief to leadership addressing outcomes, concerns, and ways forward.

Figure 5 Investigation and Post-Incident Activity (Phase IV)

4.4 Organization

To adequately respond to an incident, established teams participate depending on incident characteristics. As situation develops and its impact becomes significant, various teams may be called to contribute. Figure 6 depicts Organization IR organization.

4.4.1 Escalation Levels

Incident escalation increases as severity increases to involve appropriate resources. Incidents are handled at lowest level with as few resources as necessary to reduce total impact and enable complete control. Table 4 recommends escalation levels and associated team involvement.

Table 4: Escalations

Escalation Level	**Affected Team (s)**	**Description**
0	• Users	Normal Operations. Users and engineering groups monitoring for alerts from various sources.
1	• Users • Navy Help Desk • Local Command ISSM/IRT • CO	A threat has been discovered. Determine defensive action to take. Email users of required actions, if necessary.
2	• Users • Navy Help Desk • Local Command ISSM/IRT • CO	A threat has manifested itself. Determine course of action for containment and eradication. Email users of required actions, if necessary.
3	• Local Command ISSM/IRT • CSSP (CSDO) • Navy Help Desk • CO	A threat is wide spread or impact is significant. Determine course of action for containment and eradication. Email users. Prepare to take legal action for financial restitution, etc

4.5 Incident Response Process

At each escalation level, team members who will be needed at next higher level of escalation are alerted so they will be prepared to respond if and when they are needed. Figure 7 describes the overall IR process, while section 4.5.1 outlines roles and responsibilities of individual teams.

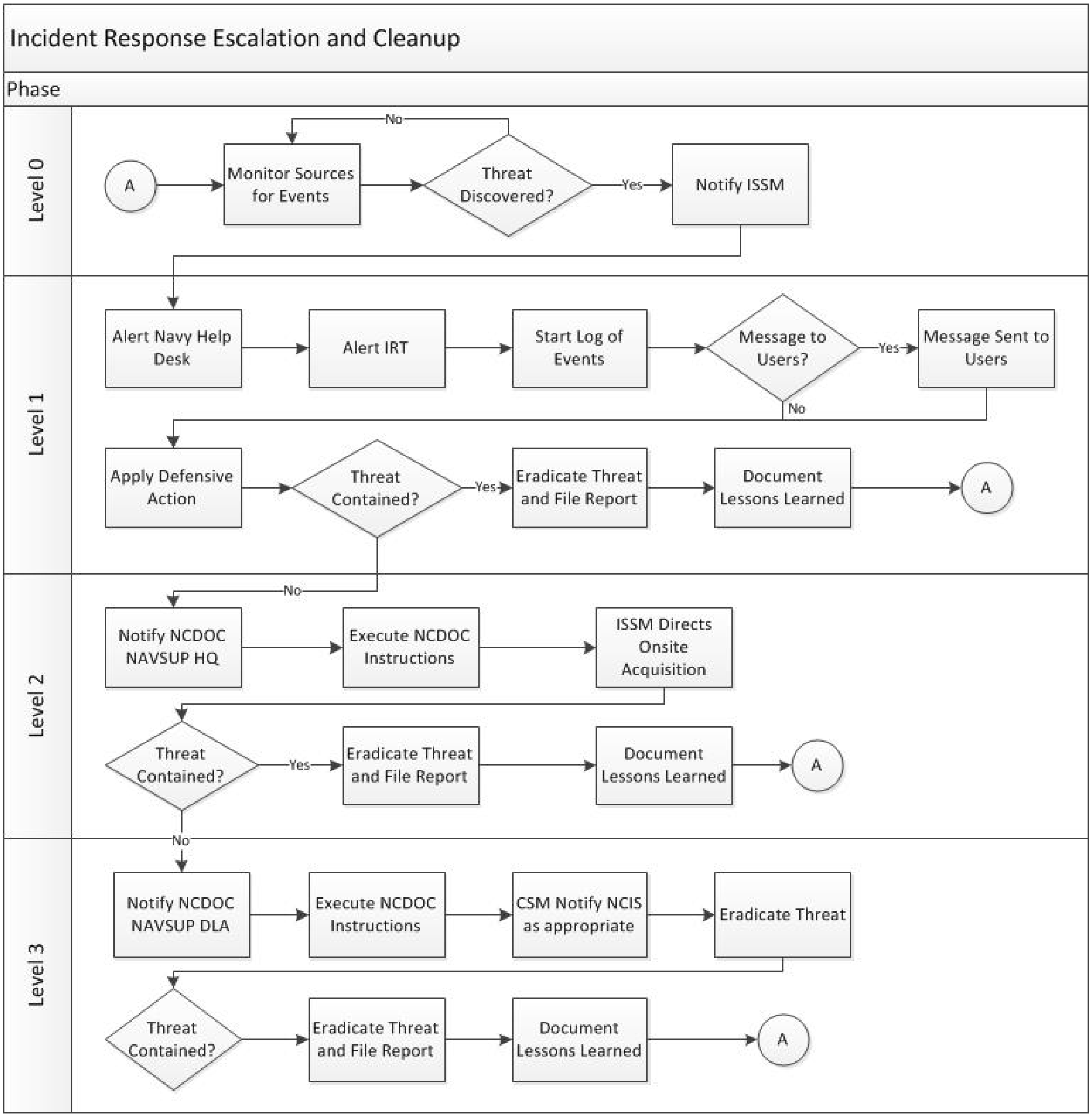

Figure 7. Incident Response Process

4.5.1 Incident Response Escalation Roles and Responsibilities

Table 5: Role Escalations and Responsibilities

Escalation Levels	**Roles**	**Responsibilities**
Escalation Level 0		
Users		1. Monitor known sources for alerts or notification of a threat.
Escalation Level 1 (*A possible threat has been discovered.)*		

Users	1. Notify appropriate POC
Technical Assessment Team	1. Determine initial defensive action required. 2. Notify local Command ISSM/IRT. 3. Notify system Help Desk
Incident Response Manager	1. Receive and track reported potential threats. 2. Escalate IR to Level 2 if reports indicate a threat has manifested itself. 3. Determine relevant membership of Technical Assessment and Technical Support teams. 4. Alert IT engineering and applicable support organizations of potential threat and defensive action required. 5. Alert IR Management of potential threat. 6. Email users of required action, if necessary.
Escalation Level 2 (*threat has manifested itself.)*	
Incident Coordinator	1. Notify IR Management about threat manifestation. 2. Alert IR Support Team of incident. 3. Alert Extended Team. 4. Receive status from Technical Assessment Team and report to IRM. 5. Start a chronological log of events.
Technical Assessment Team	1. Determine best actions for incident containment. 2. Notify Technical Support Team of required actions. 3. Report status and actions taken to IR Coordinator.
Incident Response Manager	1. Assume responsibility for directing incident response activities. 2. Determine appropriate Escalation Level 3. Determine when risk is mitigated to an acceptable level. 4. Inform Organization users of incident at IR Management request. 5. Inform Organization users of necessary action, as requested by Technical Assessment Team and IR Management.
FOR OFFICIAL USE ONLY 23 Technical Support Team	1. Take action, as directed by Technical Assessment Team. 2. Report actions taken, personnel involved, and relevant details to Incident Coordinator for chronological log.
Escalation Level 3 (*threat has become widespread or has become a high severity level.)*	
Incident Response Manager	1. Notify local Command ISSM\IRT to establish communication between IRT Managers and Technical Support Team. 2. Coordinate with appropriate Department of Navy (DON) reporting commands. 3. Alert Extended Team of incident and severity level. 4. Determine when risk is mitigated to an acceptable Level. 5. Report status to Executive Management. 6. Inform Organization users, as directed by IR Management.

Extended Team (NCIS, CSDO, etc.)	1. Contact local authorities, if appropriate. 2. If local authorities are called in, make access arrangements to command center. 3. Ensure required information is collected to support legal action or financial restitution.
Incident Response Coordinator	1. Maintain a chronological log of events. 2. Post numbered status messages in incident voicemail box to provide Organization Executive Management a chronological status.
Technical Assessment Team	1. Monitor known sources for alerts, looking for further information or actions to be taken to eliminate threat. 2. Report status to IR Coordinator for chronological log of events. 3. Monitor effectiveness of actions taken and modify as necessary. 4. Report status to IR Management on progress of threat remediation and action effectiveness.
Technical Support Team	1. Act to eradicate threat, as directed by IR Management and Technical Assessment team. 2. Report actions taken, personnel involved, and relevant details to IR Coordinator for chronological log.

4.6 Navy Cyber Defense Operations Command (CSDO) Reportable Incidents

Incidents that have actual or potentially adverse effects on DON information or ISs are reported to CSDO. ISs include Navy/Marine Corps Intranet (Intranet), legacy, or other military, government, or commercial networks. Incidents include malicious logic detection and response, intrusion, attempted intrusion, probes, denial of service attacks, or technical vulnerabilities that may be exploited at a government, military, or other sites of interest. Technical vulnerabilities do not include those caused by improper configuration or application software vulnerabilities specific to a particular site. If intrusion is identified as a virus countered by DOD Antivirus software, the user or Network Security Team shall report incident to Command ISSM. ISSM shall report actual infections immediately. If an intrusion is identified as a new virus that is not eradicated by DOD Antivirus software, ISSM will immediately report the incident to CSDO. If intrusion is a technical vulnerability that may have wide exploitability, a user will report incident to ISSM, who then reports it to CSDO.

4.7 Incidents Reportable to Naval Criminal Investigative Service (NCIS)

Incidents involving suspected criminal activity such as IS trespassing, theft, unauthorized alteration of official data, data destruction, or espionage, including attempts to commit these crimes, requires reporting to NCIS. A user will report such incidents to the appropriate POC. ISSM shall report incidents to CSM, who will contact local NCIS office in accordance with applicable directives.

4.8 Response Timeframes

After an incident is identified, Organization personnel will utilize following guidance to report an incident or event (Reference (a)).

Table 6: Reporting Timelines

Category	**Description**	**Impact**	**Initial Notification to Next Tier**	**Initial Notification to Next Tier**	**Initial Submission to Command/JCD**	**Minimum**
0	**Exercise or Red Team Activity**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**
1	**Root Level Intrusion (Incident)**	High Moderate Low	< 15 min. < 8 hrs. < 12 hrs.	< 4 hrs. < 12 hrs. < 24 hrs.	< 6 hrs. < 12 hrs. < 12 hrs.	Tier 1
2	**User Level Intrusion (Incident)**	High Moderate Low	< 15 min. < 8 hrs. < 12 hrs.	< 4 hrs. < 12 hrs. < 24 hrs.	< 6 hrs. < 12 hrs. < 12 hrs.	Tier 1
3	**Unsuccessful Activity Attempt (Event)**	Any	< 4 hrs.	< 12 hrs.	< 24 hrs.	Tier 2
4	**Denial of Service (Incident)**	High Moderate Low	< 15 min. < 8 hrs. < 12 hrs.	< 4 hrs. < 12 hrs. < 24 hrs.	< 6 hrs. < 12 hrs. < 12 hrs.	Tier 1

5.0 POLICY REVIEW

The Fantastic Incident Response Plan (IRP) must be reviewed annually by (at a minimum) the ISSM, ISSO, and IRT. Changes to this document must be routed to the BComm Commander for signature.

The latest version of Fantastic Incident Response Plan (IRP) must be disseminated at a minimum to the ISSM, ISSO, IRT, and System Owner and will be made publicly available via www.thisiswheretheplanlives.gov.

DURKAJ.EMMITT.ALLEN.12345678

Digitally signed by DURKAJ.EMMITT.ALLEN. 1234567890
Date: 2021.02.21 18:08:30 -05'00'

High Chancellor of Security (HCoS),

Emmitt Durkaj
555-555-5555

Appendix A: Computer Network Defense (CND) Overview

Incident Handling Program

Organization Incident Handling (IH) Program is a component of overall CND strategy for DOD. In accordance with references (a) through (h). IH Program aligns with three services of CND:

- Protect
- Monitor, Analyze, and Detect
- Respond

Incident Handling

Incident handling is coordinated among and across DOD organizations and sources outside of DOD such as law enforcement (LE), counterintelligence (CI), intelligence community (IC), and defense industrial base (DIB) partners to protect interests of national security. This IRP draws relationships between these entities to foster a common process understanding by those responsible to direct and coordinate IR efforts.

Trend Analysis

ISSM/IRT assists CSDO CSSP incident handlers, as requested, with trend analysis. Trend analysis promotes cyber security trend awareness by accurately characterizing reported incident relationships as observed by affected parties. It is based on previously reported incident information and correlating other identified incidents when analyzing data.

Computer Network Defense (CND) Framework

CND Framework is the basis for actions taken within DOD to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD ISs and computer networks. CND protection employs CS principles to take deliberate actions in response to a CND alert or threat. DOD CND is organized into three tiers.

Tier One (Global)

This tier provides DOD-wide CND operational direction and support to Commands, Services and Agencies (C/S/A) and field activities. Tier One entities include United States Strategic Command (USSTRATCOM) and supporting entities such as Joint Task Force Global Network Operations (JTF-GNO), Defense Criminal Investigative Organization (DCIO), and National Security Agency (NSA)/Central Security Service (CSS) Threat Operations Center (NTOC). U.S. CYBERCOM is Navy Tier One.

Tier Two (Regional/Theater)

Tier Two provides DOD component-wide operational direction or support and responds to Tier One direction. Tier Two includes C/S/A and field activity cybersecurity service provider (CSSP) designated by component heads to coordinate component-wide CND. Navy Tier Two CSSP is CSDO.

Tier Three (Local)

Tier Three provides local operational direction or support and responds to Tier 2 direction. Tier Three includes bases, posts, camps, stations, and entities responding to direction from a Tier Two

CSSP to manage and control ISs, networks and services either deployed or fixed at DOD Installations. Organization IRP is local Tier Three CSSP.

Computer Network Defense (CND)

CND services define actions employed to prevent or reduce computer network attacks that disrupt, deny, degrade, destroy, exploit, allow unauthorized access to or facilitate information theft from computer networks, ISs, or their contents. A fourth area, Capability Sustainment, reflects actions that a component or its designated CSSP must perform to ensure provided services. C/S/As and field activities must acquire CND services through service relationships with CSSPs.

Before an Attack

Before an attack, ISSM and IRT should prepare and train for the next incident. This includes regular exercises, both simulated and tabletop, to prepare the team. IRP should train to improve team skills in both incident handling and data acquisition.

During an Attack

If attack or incident is cyber related, begin logging event, start process described in Section 4.3.2, and complete Appendix B.

Once an attack is categorized, appropriate checklist (Appendix E Category 1 & 2 Root Level and User Level Intrusion, Appendix F Category 4 Denial of Service Attack, and Appendix G Category 7 Malicious Logic Attack) is completed to further define attack and obtain appropriate information.

A key response area is to restore system operations as soon as practical.

After an Attack

Once attack is over, develop a root cause analysis and lessons learned document. These lessons learned should be presented to command management/leadership for review and approval. Approved changes should be documented and added to the IR process.

Appendix B: Organization Reporting Procedures & Contact Information

Appendix C: Communications Plan

NAVUP BSC Points of Contact

The below table provides contact numbers for Organization ISSM staff.

Name	Title	Email	Primary Phone	Secondary
Brandon Hertel	Genius	BH@Hotmail.com	123-456-7891	N/A
Emmitt Durkaj	Alchemist	ED@NetZero.edu	555-555-5555	555-555-5555
Tara Gordan	Conqueror	TG@Vidoori.com	421-233-5454	N/A

Appendix D Incident Response & Recovery Plan for Category 1 & 2

Root Level and User Level Intrusion

1. This plan is a tool to assist commands with detection, analysis, containment, eradication, and recovery from possible computer compromise for Category 1 or 2 incidents. This is not the only incident response and recovery method. CSDO may direct additional steps based on analysis of each incident.
2. If a compromise is verified on one computer, then all computers on that network are suspect. All remaining computers need to be examined for compromise.

INCIDENT RESPONSE & RECOVERY PLAN (CAT 1&2)

Detection and Analysis

______ Examine log files for unusual connections or activity. Use Event Viewer to check for odd logon entries, service failures, or odd system starts. Check firewall, web server, and router logs if saved on a different computer.
Note: Most intruders will edit log files to hide their activity. Logs must be set to append-only media.
______ Check for odd user accounts and groups. Verify accounts and groups on network with User Manager/Computer Management Tool. Ensure built-in Guest account is disabled. Rename default administrator account. In a domain environment, disable local user accounts unless specifically required for operations.
______ Check groups for valid user membership. Some default groups give special privileges to members of those groups. Ensure accounts in these groups are accurate.
______ Check for invalid user rights and privileges. User Manager Tool is located under Policies, User Rights. Ensure appropriate user accounts are assigned appropriate rights.
______ Check for unauthorized applications that may have started. Different methods allow a back door program to run. Check startup folders for shortcuts. Check “All Users” account and user accounts.
*If a suspected compromised host is running a UNIX operating system, refer to Unix Incident Response and Recovery Plan. Latest windows versions might have new locations. Review technical documentation.
______ Check for running active services. Ensure only authorized and necessary services started. Verify what services started automatically and confirm they are necessary.
______ Check system and network services for unauthorized entries. Look for invalid settings (e.g., WINS, IP Forwarding). Use the Network Properties Tool or “ipconfig /all” command at command prompt to check settings.
______ Check for unauthorized shares. Use “net share” command from command prompt or Server Manager Tool to list shares on a system.

______ Check for scheduled jobs. Ensure that scheduled jobs are necessary and correct files/programs are directly or indirectly referenced.
______ Check for odd processes. Task Manager Tool will show currently running system processes.
______ Look for unusual or hidden files for password cracking programs, password files, Trojans, and other malware. Use “My Computer □Tools □□Folder Options □□View □Show Hidden Files and Folders” to show hidden files.

______ Check for computer policy changes. Policies define a wide variety of configurations used to control what users can and cannot do. Keep a copy of system policies to verify later.
______ After these steps are verified contact CSDO Incident Handlers or CND Watch Officer before proceeding to containment steps and provide following:
Command Points of Contact: (i.e. ISSM, ISSO, NSO, etc…)
Phone number and Email address:
When was activity discovered:
How was activity identified:
Operations impacted:
High water mark of affected host(s):
Communication Service Provider (CSP) for commands NIPRNET/SIPRNET connectivity: (i.e., NCTAMS, NAVCOMTELSTA, SPAWAR, or DISA)
CSDO will provide a Navy CIRT Database (NCD) ticket number for tracking purposes.

Containment

______ After evaluating operational impact and in coordination with CSDO CNDWO/BWC disconnect identified and suspected compromised hosts from network by removing network cable from network interface card (NIC) while leaving power applied to preserve host volatile memory.
______ Place a notification placard directing personnel not to tamper with host. Affected host should not be powered down or moved until a hard drive is image acquired.
______ Provide Mission Assurance Category (MAC) Level and operational impact as an incident result to CSDO. CSDO CNDWO will assess and determine MAC level of compromised system if unknown.
______ Gather system logs from domain controller unless it is identified as a compromised host.

Eradication & Recovery

______ Rebuild compromised system(s) from a fresh OS build. (e.g. OEM or ISNS build as applicable to Network Clemency – Intranet, IT21, Intranet).
______ Mitigate additional vulnerabilities and complete preventive measures as directed by CSDO. Upon completion of CSDO’s Cyber Forensics analysis, CSDO will provide additional mitigation actions.
______ Return affected systems to an operationally ready state upon approval from CSDO.
______ Confirm affected systems are functioning normally.

Appendix E Incident Response & Recovery Plan for Category 4