



Incident Response Policy and Plan
**The Department of Housing and Urban
Development**

Office of the Chief Information Officer

HUD Handbook 2400.35 REV1

July 2016

DOCUMENT CHANGE HISTORY

Issue	Date	Pages Affected	Description
Original	07/26/2016	All	Initial Draft Version 1.0

Table of Contents

PREFACE.....	III
1.0 PURPOSE.....	4
2.0 RESCISSION.....	4
3.0 SCOPE.....	4
4.0 APPLICABILITY.....	5
5.0 STATEMENT OF MANAGEMENT COMMITMENT.....	5
6.0 DEFINITIONS.....	5
7.0 AUTHORITIES AND REFFERENCES.....	7
8.0 OBJECTIVES AND MEASURES OF EFFECTIVENESS.....	8
8.1 STRATEGIC GOALS AND METRICS.....	10
8.1.1 INCIDENT DETECTION.....	10
8.1.2 INCIDENT DETECTION: MEASUREMENT.....	10
8.1.3 INCIDENT DURATION.....	10
8.1.3.1 INCIDENT DURATION: MEASUREMENT.....	11
8.1.4 INCIDENT PREVENTION.....	11
8.1.4.1 INCIDENT PREVENTION: MEASUREMENT.....	11
9.0 ORGANIZATION AND STRUCTURE.....	12
10.0 ROLES AND RESPONSIBILITIES.....	12
11.0 INCIDENT HANDLING.....	19
11.1 PREPARATION ACTIONS.....	19
11.2 INCIDENT DETECTION AND ANALYSIS.....	20
<i>Detection</i>	20
<i>Analysis</i>	21
<i>Incident Prioritization</i>	22
<i>Incident Documentation</i>	23
<i>Incident Notification</i>	24
11.3 CONTAINMENT, ERADICATION, AND RECOVERY.....	24
11.4 POST-INCIDENT ACTIVITY.....	25
<i>Incident Handling Checklist</i>	25
11.5 COORDINATION AND INFORMATION SHARING.....	27
11.5.1 US-CERT.....	28
12.0 VULNERABILITY MANAGEMENT.....	28
<i>Vulnerability Scanning</i>	28
<i>National Cybersecurity Assessment and Technical Services (NCATS) Vulnerability Management Process</i>	28
<i>Advisory Distribution</i>	29
13.0 INFORMATION DISSEMINATION CONTROL.....	29
14.0 INCIDENT RESPONSE POLICY AND PLAN COMPLIANCE REQUIREMENTS...	31
15.0 EFFECTIVE IMPLEMENTATION DATE.....	31

PREFACE

The Department of Housing and Urban Development (HUD) Chief Information Security Officer (CISO) has been given responsibility by the Department's Chief Information Officer (CIO) to provide leadership and guidance to all HUD program offices in the areas of security incident response planning and plan evaluation. The CISO has established the Computer Incident Response (CIRT) Team to implement the incident response program. The CIRT's goal is to establish a Department-wide incident response environment that facilitates cooperation between program offices responsible for handling security incidents that affect the Department.

This document is intended to establish a unified Departmental approach for handling security incidents within the HUD infrastructure.

This Incident Response Policy and Plan (IRPP) is a complement to the HUD IT Security Policy, *Handbook 2400.25, Section 4.9 Incident Response*.

1.0 PURPOSE

The Department of Housing and Urban Development's (HUD) CISO has established the CIRT to respond to computer incidents affecting the Department. These computer attacks may be directed against the Department's Information Systems (IS) or other computer-based assets, such as environmental control systems and physical perimeter control systems. Incidents involving cyber threats, such as viruses, malicious user activity, and vulnerabilities associated with highly interconnected technology, require a skilled and rapid response before they can cause significant damage to computing resources, loss or destruction of data, loss of funds, loss of productivity, or damage to HUD's reputation.

This Incident Response Policy and Plan (IRPP) provides incident response guidelines for implementation within HUD for all information systems, including those that process and house sensitive Personally Identifiable Information (PII). The requirements outlined in this IRPP are **mandatory**, and are designed to standardize incident handling and reporting.

This document provides:

- *the requirements for incident response handling*
- *agency objectives for incident response handling*
- *the organizational structure for incident response handling*
- *roles and responsibilities for key elements and personnel*
- *preparation and training guidelines*
- *policy for handling incidents*

2.0 RESCISSION

This IRPP supersedes any incident response planning documents published before its establishment, with the exception of HUD IT Security Policy, *Handbook 2400.25, Section 4.9 Incident Response*.

3.0 SCOPE

This Incident Response Policy and Plan (IRPP) provides mitigation strategies and responses to intentional or inadvertent information security events affecting the confidentiality, integrity, and availability of information, automated information systems and networks of HUD. The IRPP does not address physical disruptions to, or the loss of, information, automated information systems or networks as a result of manmade or natural disasters impacting the information infrastructure. These non-cyber events are normally included in a Continuity of Operations Plan (COOP) or Operations Back-up Plan.

4.0 APPLICABILITY

The provisions and guidelines of this IRPP apply to all accredited HUD information systems and non-accredited information systems (e.g. any partner organizations and systems that are provided and handle HUD data). The provisions and guidelines of this Plan also apply to all personnel who support information security incident response in any capacity. This includes, but is not limited to, end-users, help desk personnel, systems and network administrators, system owners, system developers and information security personnel. The provisions of this plan may impact, and should be coordinated with, the owners of any interfacing information, applications, automated information systems or networks identified in IAS.

5.0 STATEMENT OF MANAGEMENT COMMITMENT

The United States Department of Housing and Urban Development (HUD) is responsible for providing resources for empowering local governments, business, and organizations to build stronger communities. Part of HUD's support mission is to provide Information Technology (IT) project management planning and acquisition support; IT technical services, including software development and maintenance, as well as quality assurance support related to IT products and processes. HUD has adopted lifecycle management policies and procedures to promote the effective acquisition, development, and management of information systems. In fulfilling this support mission, HUD's IT systems process and store critical and sensitive data, including the Personally Identifiable Information (PII) of many employees and customers.

Therefore, HUD's senior leadership is committed to fulfilling the HUD Computer Incident Response Team's mission to ensure the ongoing confidentiality, integrity, and availability of the data and IT systems that are utilized to accomplish HUD's larger mission. In order to do this, HUD's CIRT must be prepared to detect, analyze, prioritize and remediate IT security incidents. The HUD IT Security Handbook 2400.25 REV4 defines a security incident as "...a violation or imminent threat of violation of information security policies, acceptable use policies, or standard computer security practices."

6.0 DEFINITIONS

CIRT – The Computer Incident Response Team administers the incident response program to include monitoring, tracking, response coordination and reporting of HUD computer security incidents. HUD-CIRT manages and responds to computer security incidents that involve HUD systems and data, to help improve the overall security posture of HUD by independently verifying the security of HUD systems, and to ensure the timely dissemination of security information to the appropriate stakeholders.

Event - Any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a potentially negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access

to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security-related, not those caused by natural disasters, power failures, etc.

Incident – A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

Major incident - A computer security incident with a confirmed impact involving one or more of the following that requires coordinated response and deviation from normal response, remediation, and recovery activities:

- One or more mission critical systems (as identified in the Inventory of Automated Systems) are affected where the functional impact was confirmed to be other than none;
- A confirmed compromise where there is a high confidence or confirmation attributed to an Advance Persistent Threat (APT) actor
- A high number of systems affected (10 or more);
- An imminent attack that has a high confidence of resulting in a functional impact of other than none (e.g., currently under escalating denial of service attack);
- An attack is spreading quickly (e.g., network aware worm);
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money; or
- A site or system is exposed to potential or actual serious damage (e.g., life threatening, financial, legal [includes confirmed large scale/ high publicity Privacy incidents])

Privacy Incident – a violation or imminent threat of a violation of privacy laws, principles, policies, and practices. Breaches, which are the loss of control, compromise, unauthorized disclosure, unauthorized access, or any similar term referring to situations where persons other than authorized individuals and for any other than authorized purpose have access or potential access to PII in usable form, whether physical or electronic. However, there are other types of privacy incidents, including using PII for purposes other than the stated purpose for which the information was originally collected, exceeding the retention period for PII, and collecting and/or using PII without first providing proper notice. The term “privacy incident” encompasses both suspected and confirmed incidents involving PII and applies in either a classified or unclassified environment. It includes information in both electronic and paper format and information maintained in a system of records as defined by the Privacy Act.¹

¹ HUD Breach Notification and Response Plan

Personally Identifiable Information (PII) - PII is not anchored to any single category of information or technology. Rather it demands a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source—that, when combined with other available information, could be used to identify an individual.

Sensitive Personally Identifiable Information (SPII) – PII that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone data elements. Some examples of SPII include biometric information (e.g., DNA, iris images, fingerprint, and photographic facial images), Social Security Number (SSN), account numbers, and any other unique identifying number (e.g., Federal Housing Administration [FHA] case number, driver's license number, or financial account number, etc.). Other data elements such as citizenship or immigration status; medical information; ethnic, religious, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also SPII.²

US-CERT - The United States Computer Emergency Readiness Team (US-CERT) is an organization within the Department³ of Homeland Security. US-CERT is responsible for analyzing and reducing cyber threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. The division brings advanced network and digital media analysis expertise to bear on malicious activity targeting the networks within the United States and abroad.

Users - Include all HUD employees and contractors, including vendors and agents that provide services and resources to HUD.

Vulnerability – A weakness in a system (e.g., system security procedures, hardware, design, or internal controls) that could be exploited.

7.0 AUTHORITIES AND REFFERENCES

Computer security incident response has been made a requirement within the Department of Housing and Urban Development as stated in the HUD IT Security Handbook 2400.25, section 4.9. The IT Security Handbook 2400.25, section 4.9.6 places a responsibility upon all HUD users to report all computer security incidents to the HUD National Helpdesk at 1-888-297-8689, in accordance with HUD Policy. These requirements for incident response and reporting are part of the Department's effort to attain the goals outlined in the National Institute of Standards and Technology Special Publication 800-61, Computer Security Incident Handling Guide.

² HUD Breach Notification and Response Plan

The following documents establish or provide the basis for establishing computer incident response within the Department:

- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*
- Federal Information Processing Standards 200 (FIPS 200), *Minimum Security Requirements for Federal Information and Information Systems*
- HUD IT Security Policy, *Handbook 2400.25*
- HUD Breach Notification Policy and Response Plan 3150.1
- Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- Federal Information Security Management Act of 2002

8.0 OBJECTIVES AND MEASURES OF EFFECTIVENESS

The Computer Incident Response Team (CIRT) has been established to protect and defend the organization’s systems and network against intrusive, abusive, and destructive behavior from both internal and external sources. To meet the aforementioned goal, the objectives and target performance metrics of the IRPP are as follows.

No.	OBJECTIVE	TARGET
1.	Proactively prepare and practice implementation of an incident response	Test the IRPP annually, or when significant personnel turnover in key positions has occurred. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.
2.	Increase the detection of incidents by HUD’s security solution	Track the source of detection of each incident. Source of incident detection metrics allow comparison of the percentage of incidents reported by users, administrators, and other parties with the percentage detected by the CIRT solution.

No.	OBJECTIVE	TARGET
3.	Initiate comprehensive record keeping immediately to ensure critical observations and technical details are captured to support evidentiary or technical analysis needs	System users, the CIRT, System Administrators initiate an Incident/Event Log upon recognition of any suspicious activity. System Administrators begin documenting and capturing system/network “snapshots” on the determination that suspicious activity reported by a user may not be related to user error or a system malfunction.
4.	Rapidly report available details to the CIRT and notify interfacing systems and network owners of suspected events and incidents	The user, program office, or IT support staff notifies the HUD National Helpdesk at 1-888-297-8689 within one hour after the incident. The HUD National Helpdesk issues an initial Incident Report in via a Service Desk ticket to the CIRT. The CIRT reports incident with a functional or informational impact to US-CERT within one hour of the impact confirmation by the CIRT in accordance with US-CERT reporting requirements.
5.	Help users and program offices limit the incident’s duration to recover quickly and efficiently	The CIRT and System Administrator provide immediate guidance to users reporting suspicious activity, and follow-up specific mitigation instructions as soon as possible.
6.	Minimize operational impacts from the loss or degradation of information, applications, systems and networks	No loss of mission capability.
7.	Minimize the exposure of PII to unauthorized persons	Reduce the impact of PII incidents with timely containment and eradication
8.	Develop systematic procedures to form a comprehensive approach based on proven techniques to ensure rapid recovery	Review and update the IRPP on an annual basis, in case of a new and significant event, and incorporate lessons learned from IRPP exercise.
9.	Carefully consider operational requirements along with analytic/forensic and legal requirements in the development of mitigation actions	No loss or compromise of data required for technical analysis or legal evidence caused by poor record keeping, unless the CIRT determines potentially serious operational consequences could result.
10.	Ensure that all security professionals are trained to HUD standards and that all personnel are prepared to identify and respond to cyber events and incidents	Full compliance with the individual and collective training standards specified in the HUD Security Awareness Training and Education Program, with respect to newcomer and refresher training for all

No.	OBJECTIVE	TARGET
		categories of personnel involved in the IR process.
11.	Immediately acknowledge and act on, as appropriate, the CIRT requests for data	Report compliance within the specified time period in the required format.

8.1 STRATEGIC GOALS AND METRICS

The HUD Office of Information Technology Security (OITS) has several strategic goals to increase the CIRT program’s capability to reduce the overall risk of IT security incidents negatively impacting the larger HUD IT support mission. These goals are both measurable and attainable. The Metrics section of this plan details the measurement of the effectiveness of HUD’s goals against the performance of the incident response program. In addition, the Roadmap section of this document outlines HUD’s plan to realize the goals HUD has defined.

8.1.1 INCIDENT DETECTION

A primary goal is to increase the detection of incidents by HUD’s security solution. Currently the majority of incidents are detected by user and system administrator reports. While user reports are helpful and desirable, mature incident detection capabilities provide the majority of incident detections for their organizations. The goal is to rely on incident handlers or security operations personnel as the primary source of incident detection.

An additional goal is to reduce the time to detect an incident. The time to detect an incident is also referred to as the dwell time. As incident detection capabilities mature, incidents will be detected much closer to the start of the activity reducing the overall dwell time. Reduced dwell time results in a reduction of overall time that incidents have to take negative actions against HUD’s IT support mission.

8.1.2 INCIDENT DETECTION: MEASUREMENT

To measure the effectiveness of HUD’s incident detection capability the CIRT will track the source of detection of each incident, and the time from incident start to detection. Source of incident detection metrics will allow HUD to compare the percentage of incidents reported by users, administrators, and other parties with the percentage detected by the CIRT solution. Once the incident detections begin to occur more reliably through the CIRT solution, tracking the average time from incident start to incident detection will measure how effectively the tool configurations and CIRT processes are at detecting incidents.

8.1.3 INCIDENT DURATION

Another goal of the HUD incident response program is to reduce the overall duration of security incidents once they are detected. Based on the current state of the HUD CIRT program, this can

be most effectively done by reducing analysis time. Creating an in-house analysis environment, adding analysis and forensic tools, standing up log aggregation and correlation capabilities, and getting network documentation and diagrams from HUD's IT vendors will drastically reduce the current analysis timeframe. Currently minimal analysis is performed by CIRT personnel in the production environment to prevent further spread of the incident. When the analysis requires more in-depth review, it is sent to the United States Computer Emergency Readiness Team (US-CERT) for further analysis. Due to US-CERT's volume of incidents, analysis results can take several weeks. With a local analysis environment, this turnaround time can be reduced to hours. In addition, incident handlers must request audit logs from HUD's IT vendors. Standing up log aggregation and correlation capabilities will reduce the time to investigate system logs. Finally, having network diagrams and documentation will allow incident handlers to more quickly identify the devices involved in incidents.

8.1.3.1 INCIDENT DURATION: MEASUREMENT

To measure the impact this Incident Response Policy and Plan has on incident duration metrics that will be tracked for average analysis time per incident, and average incident time to eradication or containment. Tracking the average analysis time measures the effectiveness of the CIRT's analysis processes and tools. Analysis time will be tracked as the time from detection of an incident to the time that containment or eradication activities begin. HUD expects to see a reduction in the overall analysis time as a direct result of the execution of this plan.

In addition, average incident time from detection to mitigation will be tracked in order to measure the overall impact of the added tools, processes, and training on the entire incident lifecycle through eradication or containment.

8.1.4 INCIDENT PREVENTION

Ultimately HUD would like to prevent the occurrence of incidents wherever possible. Security incidents can be costly to respond to and recover from. An effective incident response program takes advantage of lessons learned from previous incidents. Applying the corrective actions gained by lessons learned will reduce the overall incidents that occur in the HUD environment.

Also, as the CIRT program matures, additional capabilities like threat intelligence and defensive countermeasure development will allow incident responders and other security personnel to focus on attack precursors that will allow for prevention (or pre-mitigation) of pending attacks.

8.1.4.1 INCIDENT PREVENTION: MEASUREMENT

There will be an initial surge in total incidents due to increased detection capability. However, after a period of time the total incidents will level. Once an initial baseline is established, the total number of incidents over time will allow HUD to measure the effectiveness of incident prevention efforts.

The total number of incidents compared by threat vector will also be measured. This will allow HUD to focus the incident response program and other security initiatives at the key areas where threatening activity is observed.

9.0 ORGANIZATION AND STRUCTURE

HUD’s Incident response capability is aligned under the Office of Information Technology Security (OITS), Office of the Chief Information Officer (OCIO).

HUD has chosen to implement a “fully outsourced” and “central incident response team” per the recommendations set out in NIST SP 800-61 REV2 section 2.4.1. The team functions as a part of the HUD Security Incident Response Management Contract administered by OITS. Within OITS, a Government Technical Monitor (GTM), and a HUD Program Manager have been appointed to oversee the day-to-day operations of the CIRT. The CIRT is physically based in a federal building less than a mile from the HUD Headquarters building in Washington, DC.

The CIRT is responsible for coordination and support of all response activities. All incident response activities at the program office level must be reported to the CIRT. The CIRT can be contacted at cirt@hud.gov.

The CIRT is comprised of junior, intermediate, and senior shift analysts as well as one principle analyst that serves as the program manager and technical team lead.

10.0 ROLES AND RESPONSIBILITIES

Effective Incident Handling requires a formal delineation of organizational roles and responsibilities. This ensures that when an incident occurs, there is an agreed upon structure that will be used to determine who should be performing each step of the incident handling processes and who will provide command and control for the incident handling process.

Role	Responsibilities
Chief Information Officer (CIO) and Principal Deputy CIO	<ul style="list-style-type: none"> • Responsible for establishing and overseeing the department-wide Information Security Program • Provides information security consulting assistance to all HUD program offices for their individual programs • Appoints the CISO • Reviews and evaluates the HUD information security program annually.
Chief Information Security Officer (CISO)	<ul style="list-style-type: none"> • Directs the management of HUD’s information security program • Establishes and maintains the HUD Information Security program • Interacts with internal and external resources

	<ul style="list-style-type: none"> • Sponsors an Information System Security Forum • Coordinates security compliance across HUD’s program offices • Serves as the CIO’s primary liaison with the HUD’s authorizing officials, information system owners, and Information System Security Officers (ISSOs) • Works with the Office of General Counsel (OGC) and the Office of Inspector General (OIG) to coordinate law enforcement involvement in incidents that involve criminal activity • Coordinates all official public relations statements involving incident investigations with the Office of Public Affairs
Chief Privacy Officer (CPO)	<ul style="list-style-type: none"> • Works in close consultation with the Senior Agency Official for Privacy (SAOP), CISO and OITS regarding privacy incident handling and other privacy issues affecting IT systems. • Work with the SAOP, CISO and OITS to ensure a complete and accurate Privacy Incident Report. • Consult with the CIO, Deputy CIO, and CISO concerning privacy incident handling. • Work with the SAOP, CISO and OITS to contain privacy incidents. Work with the SAOP, CISO and OITS to assess the likely risk of harm posed by the privacy incident (e.g., Low, Moderate, or High impact) to determine who should handle the investigation, notification, and mitigation of the incident.
CIRT Principle Analyst	<ul style="list-style-type: none"> • Responsible for managing and ensuring the successful completion of all incident response activities • Responsible for ensuring the appropriate coverage is maintained and shift analysts are properly trained • Primary contact point for work assignments • Performs a variety of tasks, including acting as a liaison with upper management and other teams and organizations, defusing crisis situations, and ensuring that the team has the necessary personnel, resources, and skills
CIRT Shift Analyst	<ul style="list-style-type: none"> • Responsible for investigating and implementing all cyber incidents reported to the CIRT by HUD program offices • Perform in-depth analysis of network traffic, system logs, and malware artifacts to determine the appropriate

	<p>categorization and mitigation techniques required for each case</p> <ul style="list-style-type: none"> • Administer the incident response program to include monitoring, tracking, response coordination and reporting of HUD’s computer security incidents • Manages and responds to computer security incidents that involve HUD systems and data • Help improve the overall security posture of HUD by independently verifying the security of HUD’s systems • Ensure the timely dissemination of security information to the appropriate stakeholders
Help Desk	<ul style="list-style-type: none"> • Receive reports of security events/incidents • Report all events/incidents to the CIRT • Provide the persons reporting events/incident with guidance
Office of General Counsel (OGC)	<ul style="list-style-type: none"> • Develops security clauses, as appropriate, based on current federal and HUD policies, regulations, and guidance for HUD information systems and services in conjunction with the OITS and Office of the Chief Procurement Officer (OCPO) • Provides legal opinions, advice and services in relation to incident investigations • Works with the CISO and OIG in coordinating law enforcement involvement in incidents that involve criminal activity
Office of Information Technology Security (OITS)	<ul style="list-style-type: none"> • Issues department-wide information security policy, guidance, and architecture requirements for all HUD systems and provides oversight to ensure the policies are implemented • Develops and maintains the HUD’s information security program serving as the agency-wide principal advisor on information system security matters • Reviews and approves the processes, techniques, and methodologies planned for securing information system assets • Responsible for managing the CIRT
Office of Privacy	<ul style="list-style-type: none"> • Handles the investigation, notification, and mitigation for privacy incidents working with the CISO, OITS, and Infrastructure and Operations Office (IOO). • Makes joint decisions with the HUD Breach Notification Response Team (HBNRT) regarding the propriety of external notification to affected third parties and the issuance of a press release in Low and

	<p>Moderate-Impact privacy incidents that occurred and provide recommendations to the SAOP</p> <ul style="list-style-type: none"> • Make incident-closure recommendations in consultation with the HBNRT. • Prepare an annual report for the SAOP and CIO outlining the lessons learned from privacy incidents that occurred during the year and identifying ways to strengthen Departmental safeguards for PII and to improve privacy-incident handling
Infrastructure and Operations Office (IOO)	<ul style="list-style-type: none"> • Manages and directs HUD’S IT infrastructure that provides shared services across HUD • Ensures the implementation of security components to secure these information system assets • Works with the OGC, OIG, and CISO to coordinate law enforcement involvement in incidents that involve criminal activity • Works with the CIRT to resolve computer security incidents, includes taking certain actions within the infrastructure, e.g. deleting emails from across the agency, collecting hard drives, providing evidence, and eliminating malware, etc.
Office of Inspector General (OIG)	<ul style="list-style-type: none"> • Responsible for performing independent evaluations, investigations, and audits of internal and external federal security guidelines/regulations • Upon request, conducts computer forensic investigations • Works with the CISO and OGC in coordinating law enforcement involvement in incidents that involve criminal activity depending on the nature of the violation
Program Offices/System Owners	<ul style="list-style-type: none"> • Responsible for the successful operation of systems and ultimately accountable for the security of information systems under their purview • Responsible for implementing management, operational, and technical controls to ensure that they are effective in protecting the information and information systems under their purview • Program Offices and System Owners of major and minor applications coordinate with System Owners of General Support Systems (GSS) that host their applications so they can better determine the adequacy of those GSS security controls, and identify and implement compensating controls when the GSS controls do not meet the application’s needs

	<ul style="list-style-type: none"> Information Security responsibilities must be included in the annual performance plans.
Senior Agency Official for Privacy (SAOP)	<ul style="list-style-type: none"> Has overall responsibility for the Department’s Privacy Program Serve as chairperson of the HBNRT Serve as an advocate for privacy incident response activities in consultation with the CIO, CISO and Privacy Officer. Advise the Secretary of any issues arising from privacy incidents that affect infrastructure protection, vulnerabilities, or issues that may cause public concern or loss of credibility.
Service Providers	<ul style="list-style-type: none"> Include vendors, contractors, other federal government organizations and entities that provide IT services, information systems, and facilities housing HUD information systems Responsible for ensuring and maintaining security controls that are compliant with HUD’s Information Security policy and procedures, including reporting security incidents to the CIRT
Supervisors	<ul style="list-style-type: none"> Authorize issuance of information system access for their staff Directly responsible for notifying System Owners when staff members are terminated, transferred, or no longer need access to a system
System Administrators	<ul style="list-style-type: none"> Responsible for implementing and maintaining technical controls that enforce operational and managerial controls through mechanisms contained in the hardware, software, or firmware components of the information system Must maintain an environment that creates a strong technical foundation for enforcement of information system security
System Security Administrators (SSA)	<ul style="list-style-type: none"> Responsible for approving access to the data in an application Grants/modifies/revokes user access via the Centralized HUD Account Management Process (CHAMP)
Information System Security Officers (ISSO)	<ul style="list-style-type: none"> Responsible for ensuring that the management, operational, and technical controls for securing the information system(s) belonging to the program office are in place and effective

	<ul style="list-style-type: none"> • Serves as the principal points of contact (POCs) for information systems security and actively participate in the Information Security System Officer Forum • Responsible for all security aspects of their assigned systems from inception through disposal, as well as for ensuring system availability • Responsibility includes participation in incident handling activities • Serves as the primary POC between the CIRT and the program offices/system owners during incident response activities • Security responsibilities will be included in their annual performance plans
<p>Users</p>	<ul style="list-style-type: none"> • A broad term used for all personnel that interact with HUD information system resources either in a support function, by working directly with an information system resource (i.e., system user), or as a recipient of HUD information (i.e., information user). • HUD users have responsibility to: <ul style="list-style-type: none"> ○ Comply with information security policy and apply the defined guidance to their daily work activities. ○ Assume accountability for protecting sensitive information under their control in accordance with this policy. ○ Attend and/or participate in the annual Information Security Awareness Training. ○ Attend the required role-based security training pertaining those having a security-related role (e.g., system and network administrators). ○ Report information security incidents (e.g., virus and malicious code attacks) to the CIRT according to the established and documented procedures. ○ Cooperate with the CIRT members in the investigation of security incidents. ○ Cooperate with Information Security and Privacy Program representatives or other designated HUD Program Office personnel during security compliance reviews/audits at HUD Program Office facilities (HQ, regional, and field offices) and/or site surveys at non-HUD facilities (e.g. data centers, disaster recovery facilities, satellite facilities).

	<ul style="list-style-type: none">○ Understand and comply with HUD policies, standards, and procedures regarding the protection of sensitive HUD information assets.
--	--

11.0 INCIDENT HANDLING

The HUD CIRT is aligned with NIST SP 800-61, “Computer Security Incident Handling Guide”. NIST SP 800-61 breaks incident response into a four phase life cycle. The phases are “preparation”, “detection and analysis”, “containment, eradication, and recovery”, and “post-incident activity”.

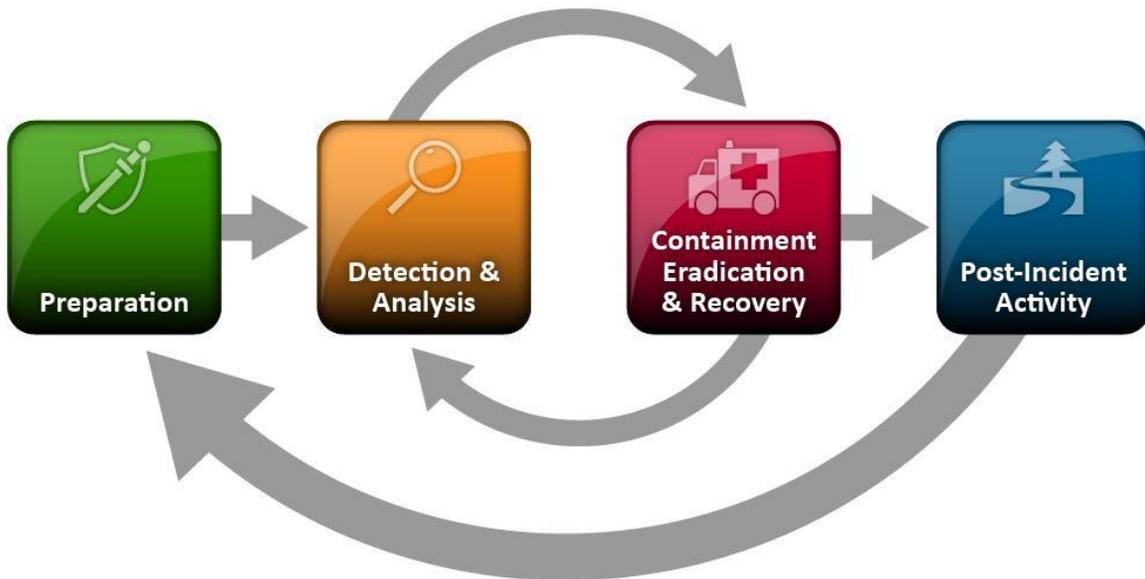


Figure 1: NIST SP 800-61 Incident Response Lifecycle

11.1 Preparation Actions

The following actions have been taken as part of this plan to attain the best possible defensive posture in advance of future cyber probes or attacks:

- HUD has provisioned Service Desk as an issue tracking system for tracking incident information and status. Service Desk is used in the incident tracking processes by the CIRT members, IT Service Providers, Privacy Office, OITS, and IOO. This platform allows for the various groups involved in the incident handling processes to coordinate and track actions taken in response to security incidents.
- HUD employs anti-virus and anti-spyware software throughout the HUD IT environment. IT service providers and the CIRT members review anti-virus logs and respond to alerts.
- HUD users are made aware of security policies and procedures regarding the appropriate use of networks, systems, and applications. All HUD users sign, and annually review the HUD Rules of Behavior document that contains statements defining appropriate use. The rules of behavior also state that users must report potential security incidents.
- HUD has a security awareness and training program that routinely provides information to users about appropriate use of networks, systems, and applications, as well as general awareness for common security threats they may encounter.

- HUD has provisioned the CIRT to be available 24/7. CIRT staff are on site for a day shift (07:00-15:00) and an evening shift (15:00-23:00), Monday through Friday, except federal holidays, with a smartphone monitored during all other times.
- Periodic risk assessments are performed on the CIRT capability against federal standards and HUD policy to ensure the effectiveness of HUD's incident response capability.

11.2 Incident Detection and Analysis

Detection

The most important first step is to recognize that an incident may be unfolding. Early recognition allows a rapid and informed identification of the nature and scope of the incident. The earlier mitigation strategies can be applied, the more likely they are to be successful.

Signs of an incident fall into one of two categories: precursors and indicators. A precursor is a sign that an incident may occur in the future. An indicator is a sign that an incident may have occurred or may be occurring now. While incidents and events can present a variety of "signs", some of the most common are:

Precursors:

- Web server log entries that show the usage of a vulnerability scanner
- An announcement of a new exploit that targets a vulnerability of the organization's mail server
- A threat from a group stating that the group will attack the organization.

Indicators:

- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.
- Antivirus software alerts when it detects that a host is infected with malware.
- A system administrator sees a filename with unusual characters.
- A host records an auditing configuration change in its log.
- An application logs multiple failed login attempts from an unfamiliar remote system.
- An email administrator sees a large number of bounced emails with suspicious content.
- A network administrator notices an unusual deviation from typical network traffic flows.

HUD leverages multiple sources for incident detection. Intrusion Detection Systems (IDSs) are maintained at the perimeter of the network and monitored by US-CERT, and HUD's IT service providers. Statistics from the IT service provider IDSs are forwarded to the CIRT weekly for review and consolidation. System logs are maintained and reviewed by HUDs IT service providers and program offices. The HUD IT Security Policy, *Handbook 2400.25, Section 5.3.11 a. Audit Record Retention* requires retention of these logs for at least one year. Security logs are captured for network devices, appliances, perimeter control devices, firewalls, Internet proxies, and servers. The CIRT and HUD IT service providers monitor publicly available bulletins from product vendors and others about new vulnerabilities and exploits in order to keep up with current trends. The CIRT specifically monitors the National Vulnerability Database (NVD) and attends the weekly US-CERT Security Operations Center (SOC) call to learn about emerging threats and

trends. Users are expected and required to report suspicious activity to the HUD National Helpdesk at 1-888-297-8689. The Helpdesk routes reports that contain potential security threats to the CIRT for further analysis.

Analysis

Incident analysis is required to determine whether incidents were detected accurately (are not false-positives), and to obtain as much information about the incident as possible. Having a wealth of information about an incident allows for proper containment, eradication, and recovery decisions.

HUD has established a log retention policy of at least one year in the HUD IT Security Handbook 2400.25. These logs are often initially reviewed by the IT service provider, or program office responsible for the system. Once there is concern of potential incident detection, these logs are made available to the CIRT for review. The CIRT reviews the logs to determine whether an incident has occurred, what the extent of the incident is, and what actions are necessary to contain, eradicate, and recover from the incident. In addition, the CIRT requests additional logs from IT service providers and program offices to further investigate incidents that are already being tracked by the CIRT. The CIRT correlates logs from different sources to try to obtain the most accurate picture of what occurred during the incident.

HUD employs the Network Time Protocol (NTP) from a Stratum-1 time server to ensure that the time of log entries is consistent across all platforms. This aids in the log correlation process and ensures the time of events is tracked and reported accurately.

The CIRT uses a knowledge base to document information they have gathered that may prove to be useful in future incident analysis. Some examples of things included in the knowledge base are:

- Points of contact
- Common issues handlers face
- Common cyber threats faced by the organization
- Common responses to threats
- Path/location of critical system files or logs

Having complete incident information readily available reduces analysis time, and speeds containment, eradication, and recovery efforts. The CIRT also uses several Internet search engines and tools for research during their analysis.

The CIRT also contacts US-CERT when necessary to request assistance with analysis. HUD has a Federal Network Authorization on file with US-CERT. This authorization allows the US-CERT Digital Analytics Branch (DAB), and Incident Response Team (IRT), to mobilize to HUD promptly to provide assistance with major incidents.

Incident analysis activities and findings are documented in the incident ticket in Service Desk.

Incident Prioritization

Incidents are not worked on a first-come, first-served basis at HUD. Security Incidents are prioritized, with major incidents having the highest priority. In general, HUD follows US-CERT's incident prioritization guidelines based primarily on functional impact. US-CERT's incident prioritization guidelines are based on impact to system function, impact to and/or loss of information, and what the overall effort is required to recover from the incident. These categories can also be found in NIST SP 800-61 section 3.2.6:

- **Functional Impact of the Incident** - Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems. Incident handlers should consider how the incident will impact the existing functionality of the affected systems. Incident handlers should consider not only the current functional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained.
- **Information Impact of the Incident** - Incidents may affect the confidentiality, integrity, and availability of the organization's information. For example, a malicious agent may exfiltrate sensitive information. Incident handlers should consider how this information exfiltration will impact the organization's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertained to a partner organization.
- **Recoverability from the Incident** - The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances it is not possible to recover from an incident (e.g., if the confidentiality of sensitive information has been compromised) and it would not make sense to spend limited resources on an elongated incident handling cycle, unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an incident may require far more resources to handle than what an organization has available. Incident handlers should consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.

Impact Classifications	Impact Description
Functional Impact	HIGH – Organization has lost the ability to provide all critical services to all system users.
	MEDIUM – Organization has lost the ability to provide a critical service to a subset of system users.
	LOW – Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance.

	<p>NONE – Organization has experienced no loss in ability to provide all services to all users.</p>
Informational Impact	<p>PROPRIETARY – The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCI), intellectual property, or trade secrets was compromised.</p>
	<p>PRIVACY – The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised.</p>
	<p>INTEGRITY – The necessary integrity of information was modified without authorization.</p>
	<p>NONE – No information was exfiltrated, modified, deleted, or otherwise compromised.</p>
Recoverability	<p>REGULAR – Time to recovery is predictable with existing resources.</p>
	<p>SUPPLEMENTED – Time to recovery is predictable with additional resources.</p>
	<p>EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed.</p>
	<p>NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).</p>
	<p>NOT APPLICABLE – Incident does not require recovery.</p>

Table 2: US-CERT Impact Classifications

Incident Documentation

If HUD CIRT suspects that an incident has occurred, they immediately start recording all facts regarding the incident. Only the facts regarding the incident, not personal opinions or conclusions are recorded. Subjective material is presented in incident reports, not recorded as evidence.

CIRT members, IT Service Providers, Privacy Office, OITS, and IOO maintains records about the status of incidents, along with other pertinent information. Tracking incidents in Service Desk helps ensure that incidents are handled and resolved in a timely manner. Service Desk contains information on the following:

- The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
- A summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Impact assessments related to the incident
- Contact information for other involved parties (e.g., system owners, system administrators)
- A list of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken (e.g., rebuild the host, upgrade an application).

Incident Notification

Incidents that have a functional or informational impact other than “none” must be reported to US-CERT within one hour of the CIRT’s confirmation of impact. The CIRT also sends notifications to key HUD stakeholders via email. This notification is in accordance with the HUD Breach Notification Policy and Plan. The HUD stakeholders that receive notifications are:

- Chief Information Security Officer
- Chief Privacy Officer
- Office of Privacy
- Office of Information Technology Security
- IT Service Providers
- Computer Incident Response Team
- Deputy CIO for Infrastructure and Operations Office

11.3 Containment, Eradication, and Recovery

Most incidents require containment, and it is an important step in ensuring an incident is prevented from overwhelming resources and/or increasing damage. In general, containment is a decision-making process.

Once analysis has reached a point where a determination is made that there are appropriate actions that can be taken to reduce the residual risk of an incident, the CIRT requests that program offices and IT service providers quickly take actions necessary to contain the incident. In the request the CIRT provides specific recommended actions to contain the incident, and requests follow-up confirmation that the containment actions have been completed.

Evidence is collected during the course of incident investigation primarily for the purpose of resolving the incident. However, evidence may be needed for future legal proceedings. Incident evidence collected during investigations is maintained for at least one year.

After containment has been fully accomplished, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. Often, eradication is either not necessary or is performed during recovery.

The CIRT requests eradication and recovery actions from the IOO and program offices as procedural steps subsequent to containment actions. Priority of eradication and recovery steps is taken into account based on the impact of each step to the overall incident recovery. The early phases of eradication and recovery focus on quick/high value changes to prevent future incidents. The latter phases overlap more with the post-incident activity and lessons learned activities, and focus on longer-term changes.

11.4 Post-Incident Activity

Post-Incident Activity consists of using the information gathered during the incident response lifecycle to feed preparation for future incidents. Some of the information can be used to prevent future incidents, while other information can be used to strengthen the incident response capabilities in the future.

The CIRT provides “Lessons Learned” documents after major incidents to formally capture lessons observed during the incident handling processes, and recommendations for improvements to the IT environment, configurations, processes, and procedures as appropriate. In preparation for capturing lessons learned, the CIRT may facilitate a lessons learned meeting involving all key incident stakeholders for a collaborative information gathering session. These sessions allow lessons to be captured from many different perspectives.

Lessons learned also feed the HUD Security Awareness and Training program, allowing OITS to target awareness activities to specific topics that have proven to impact HUD based on previous incidents.

Collected incident data is also used for FISMA reporting and other audits and evaluations as required, providing insight to incident response activities at the federal level.

Incident Handling Checklist

The checklist in table below provides the major steps to be performed in the handling of an incident. Note that the actual steps performed may vary based on the type of incident and the nature of individual incidents. For example, if the handler knows exactly what has happened based on analysis of indicators (Step 1.1), there may be no need to perform Steps 1.2 or 1.3 to

further research the activity. The checklist provides guidelines to handlers on the major steps that should be performed; it does not dictate the exact sequence of steps that should always be followed.

Action		Completed
Detection and Analysis		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	

7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Table 2: NIST SP 800-61 Incident Handling Checklist

11.5 Coordination and Information Sharing

Communication is a key part of incident response activities. The HUD CIRT communicates within and outside of HUD as a part of incident handling and information sharing activities. Much of the internal communication occurs through HUD’s incident tracking system, Service Desk. The Service Desk tickets are the CIRT’s primary method of incident documentation and coordination. However, phone and email communication are also used throughout the course of an incident.

For incident handling, the CIRT receives incident reports from IT vendors, users, and US-CERT. The CIRT also communicates with IT vendors for collection of logs and other data required for incident analysis. Interviews of end users are conducted by the CIRT when necessary after incidents have been reported. Further communication occurs with HUD’s IT vendors once containment and eradication actions are necessary. This involves the HUD CIRT providing guidance to the IT vendor on how to best contain, eradicate, and recover from the incident.

The HUD CIRT also communicates with the HUD Privacy Office when incidents involve the exposure, or potential exposure, of sensitive personally identifiable information (PII). The HUD CIRT immediately notifies the Privacy Office of any incidents that are suspected to involve a loss of PII via email. Service Desk incident tickets are used to route the details of the incident, through the containment and eradication of the PII, to the Privacy Office. The purpose of transferring Service Desk tickets to the Privacy Office is to allow for tracking of notifications and any other actions required after the initial containment and eradication has been completed.

Sometimes incidents must be turned over to law enforcement and/or addressed to the media. The HUD CIRT reports these cases to the Office of Information Technology Security recommending that the Office of the Inspector General (OIG), Office of the General Counsel (OGC), or Office of

Public Affairs be contacted as appropriate. Incidents that have a potential criminal² nature are turned over to the OIG as soon as this determination is made.

The HUD CIRT feeds information back into the OITS office by providing lessons learned, security advisories, and other technical consultation. This input provides opportunities for enhanced and targeted security awareness training and policy updates.

11.5.1 US-CERT

The HUD CIRT communicates external to HUD primarily via US-CERT. The HUD CIRT follows the US-CERT Federal Incident Notification Guidelines that can be found at www.us-cert.gov. These guidelines involve reporting incidents in a timely fashion, based on incident type. All incidents that have a confirmed impact to confidentiality, integrity, or availability are reported within one hour of confirmation in accordance with the US-CERT notification guidelines. Additionally, US-CERT generally facilitates any required communication with other government incident response teams. US-CERT also hosts a weekly meeting to discuss current trends and indicators with all of the incident response teams under its purview.

The US-CERT Government Forum of Incident Response and Security Teams (GFIRST) is a group of technical and tactical practitioners of security response teams responsible for securing government information technology systems. CIRT members are required to join GFIRST to obtain sensitive and time-critical vulnerability, security, and incident information which is disseminated to the appropriate HUD personnel in order to mitigate risks affecting the HUD environment. The GFIRST portal contains a secure email feature which is used to securely communicate (at the unclassified level) with other GFIRST members and US-CERT.

12.0 VULNERABILITY MANAGEMENT

Vulnerability Scanning

Vulnerability scans identify vulnerabilities present on the HUD network with the goal to remediate to prevent exploitation. Vulnerability scanning is performed after business hours. Due to network and application availability concerns, scanning during production hours requires written authorization from the Chief Information Security Officer.

The CIRT scans for vulnerabilities on a continual basis. Network scanning (to include authenticated patch scanning) is performed routinely and upon request. Targeted scanning of HUD systems is performed at the request of the CISO/OITS and program offices.

The results of network and targeted scan findings are prepared in a report format and then delivered to the appropriate recipients.

National Cybersecurity Assessment and Technical Services (NCATS) Vulnerability Management Process

The current vulnerability management process involves discovery, categorizing, responding and mitigating the vulnerabilities found in the NCATS scan report. Due to regulatory compliance mandates, vulnerability management has always been increasingly important to management at HUD.

Advisory Distribution

The CIRT issues advisories to other IT groups within HUD regarding new vulnerabilities and threats. The CIRT monitors for important vulnerability advisories that are applicable to the HUD network environment. Monitoring sources include the public US-CERT website, the US-CERT Government Forum of Incident Response and Security Teams (GFIRST) Portal website, various software vendor websites, the National Vulnerability Database (NVD) maintained by NIST, and various third-party vulnerability databases.

13.0 INFORMATION DISSEMINATION CONTROL

Since incident reports reveal sensitive information about the vulnerabilities, capacity to respond and operational readiness, rules for dissemination and handling controls are necessary.

HUD is currently in the process of adopting US-CERT’s Traffic Light Protocol (TLP) for distribution of incident related information. TLP is a set of designations used to ensure that sensitive information is shared with only the correct audience. It uses four different colors to indicate different degrees of sensitivity and the corresponding handling guidance.

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.
--------------	--	---

14.0 INCIDENT RESPONSE POLICY AND PLAN COMPLIANCE REQUIREMENTS

Given the extraordinary importance that proper implementation of this Incident Response Policy and Plan holds for mission performance and readiness, failure to execute the provisions of this plan through negligence or willful disregard may result in adverse administrative or disciplinary action. Refer to the HUD IT Security Policy, *Handbook 2400.25, Section 4.1.8 Personnel Sanctions* for additional information.

15.0 EFFECTIVE IMPLEMENTATION DATE

The date of issuance of this policy.