



Cybersecurity Incident Response Plan

U.S. Department of Housing and Urban Development

July 2020



Cybersecurity Incident Response Plan

Solution Information

Information	
Solution Name	<i>Cybersecurity Incident Response Plan</i>
Solution Acronym	<i>IR Plan</i>
Project Cost Accounting System (PCAS) Identifier	<i><PCAS Identifier></i>
Document Owner	<i>SOC / CIRT</i>
Primary Segment Sponsor	<i>Office of Information Technology Services</i>
Version/Release Number	<i>2.0</i>

Document History

Release No.	Date	Author	Revision Description
1.0	14-May-2020	OITS	Plan establishment
1.1	20-May-2020	OITS	Updated Contact List
2.0	15-Jul-2020	OITS	Updated IR Flowcharts Tools/Technology Appendix IOO updates



Table of Contents

Solution Information	2
Document History	2
1. Purpose and Scope	4
2. Organization and Structure	4
2.1 Roles and Responsibilities	5
2.2 Coordination and Information Sharing	5
3. Incident Taxonomy and Data Flow	7
3.1 Incident Definition	7
3.2 Incident Data Flow	7
3.3 Incident Data Elements to Record	7
3.4 Sensitive Data	13
4. Incident Response Framework	14
4.1 Prepare	16
4.2 Detect	18
4.3 Analyze	19
4.4 Respond	21
4.5 Recover	23
4.6 Review	24
5. Incident Reporting Requirements and Metrics Maintenance	26
5.1 CISA	27
5.2 Congress	28
6. Plan Testing and Maintenance	28
Appendix A. Security Operations Roles and Responsibilities	30
Appendix B. Contact List	35
Appendix C. Incident Response Framework Data Elements	36
Appendix D. Log Artifact Checklist	39
Appendix E. SOC Tools & Technologies Listing	41
Appendix F. Post-Incident Analysis Report Template	43
Appendix G. Lessons Learned Template	45
Appendix H. Authorities and References	46
Appendix I. Glossary / Definitions	47
Appendix J. Acronyms	50



Cybersecurity Incident Response Plan

1. Purpose and Scope

This Cybersecurity Incident Response (IR) Plan supports and complements the Department of Housing and Urban Development (HUD / Department) Information Technology (IT) Security Policy Handbook 2400.25 Revision 5.0 and HUD Security Operations Center Concept of Operations. This IR Plan complies with Office of Management and Budget (OMB) Circular A-130 and the Federal Information Security Modernization Act (FISMA) of 2014. It defines processes, communications, roles, and responsibilities for effectively managing cybersecurity incidents and provides guidance on the proper handling and reporting of those incidents.

The HUD Chief Information Security Officer (CISO) is responsible for cybersecurity incident management (IM), planning, response, and plan evaluation. A computer incident within the Federal Government as defined by the National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2 is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

The purpose of this IR Plan is to enable the HUD Security Operation Center (SOC) to prepare, detect, analyze, respond, recover, and review cybersecurity incidents on HUD information systems. This IR Plan is applicable to HUD employees, contractors, and information systems except for the HUD Office of the Inspector General (OIG). This IR plan is intended to be a living document. It will be amended annually to improve and refine IR processes so that the SOC can continue to effectively respond to cybersecurity incidents and proactively adapt to an evolving threat landscape.

2. Organization and Structure

The SOC aligns under the Office of Information Technology Services (OITS), Office of the Chief Information Officer (CIO). The SOC is comprised of four cross-functional capabilities: Incident Management (IM), Threat Management (TM), Threat Intelligence (TI), and Attack Surface Reduction (ASR), and is supported by a Security Engineering function that oversees the SOC's underlying technical architecture. IM governs IR activities through the Cyber Incident Response Team (CIRT). The CIRT analyzes, validates, and responds to suspected cybersecurity incidents, and disseminates incident information to key HUD stakeholders. The orchestration and collaboration of the SOC IM, TM, TI, and ASR functions work hand in hand to rapidly detect, analyze, respond, and recover from cybersecurity incidents. See Figure 1 for an organizational view of the HUD SOC.



Cybersecurity Incident Response Plan

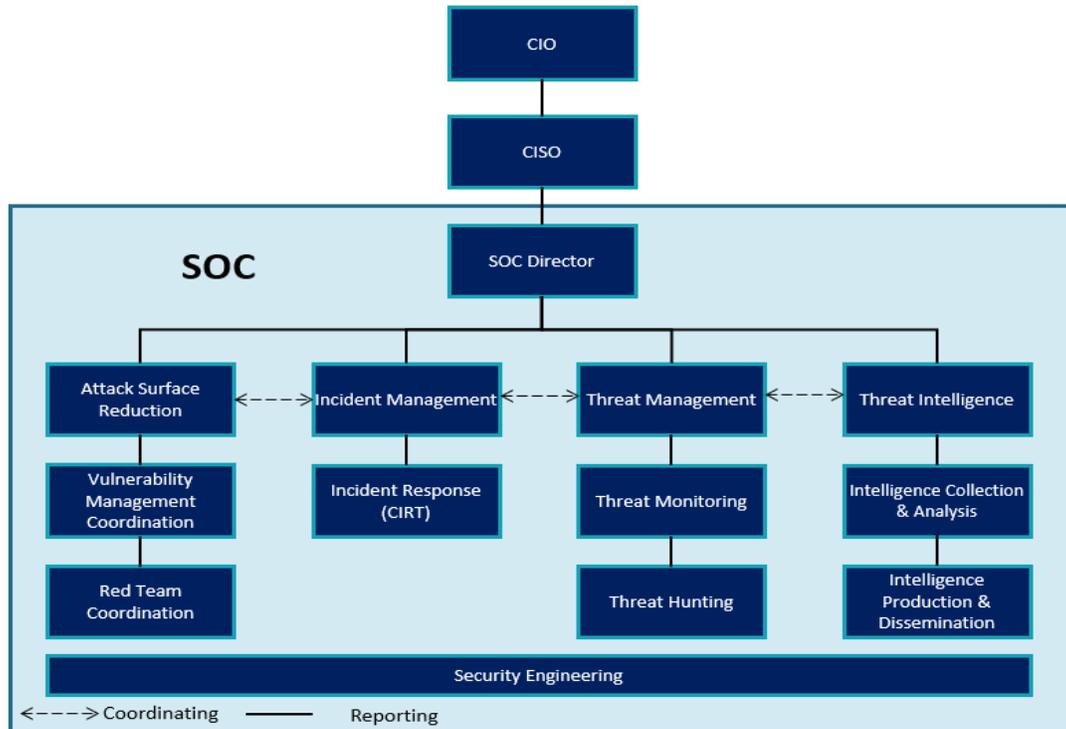


Figure 1: HUD SOC Structure

2.1 Roles and Responsibilities

The implementation and effectiveness of the IR Plan ties into stakeholder adherence to assigned roles and responsibilities. Appendix A details the full listing of roles and responsibilities of all stakeholders involved in the implementation of the SOC IR Plan:

- Secretary of HUD
- Chief Privacy Officer (CPO)
- CIO and Principal Deputy CIO
- CISO
- Office of General Counsel (OGC)
- OITS
- Office of Privacy
- Infrastructure and Operation Center (IOO)
- OIG
- Senior Agency Official for Privacy (SAOP)
- SOC Director
- Incident Commander
- IM Lead
- IM Team
- TM Team
- TI Team
- ASR Team
- CIRT
- HUD Breach Notification Response Team (HBNRT)
- Supervisors
- System Administrators
- Information System Security Officers (ISSO)
- Service Providers
- Help Desk
- Users

2.2 Coordination and Information Sharing

HUD IM through HUD CIRT shares information and coordinates IR and recovery activities. HUD CIRT receives cybersecurity incident reports from HUD’s IT system owners and providers, network users, and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). HUD CIRT communicates and coordinates with HUD’s IT



Cybersecurity Incident Response Plan

system owners who directly maintain and operate HUD infrastructure for the collection of logs and other data required for incident analysis. End user interviews should be conducted by HUD CIRT when necessary after incidents have been reported. Further communication occurs with HUD’s IT system owners once containment and eradication actions are necessary. HUD CIRT will provide guidance to the system owner(s) on how to contain, eradicate, and recover from the incident.

Figure 2 illustrates the communications flow from event detection to incident recovery. It also depicts major stakeholders who will be notified of a HUD cybersecurity incident depending on incident impact and severity. More detailed IM workflows can be found in Section 4 of this document.

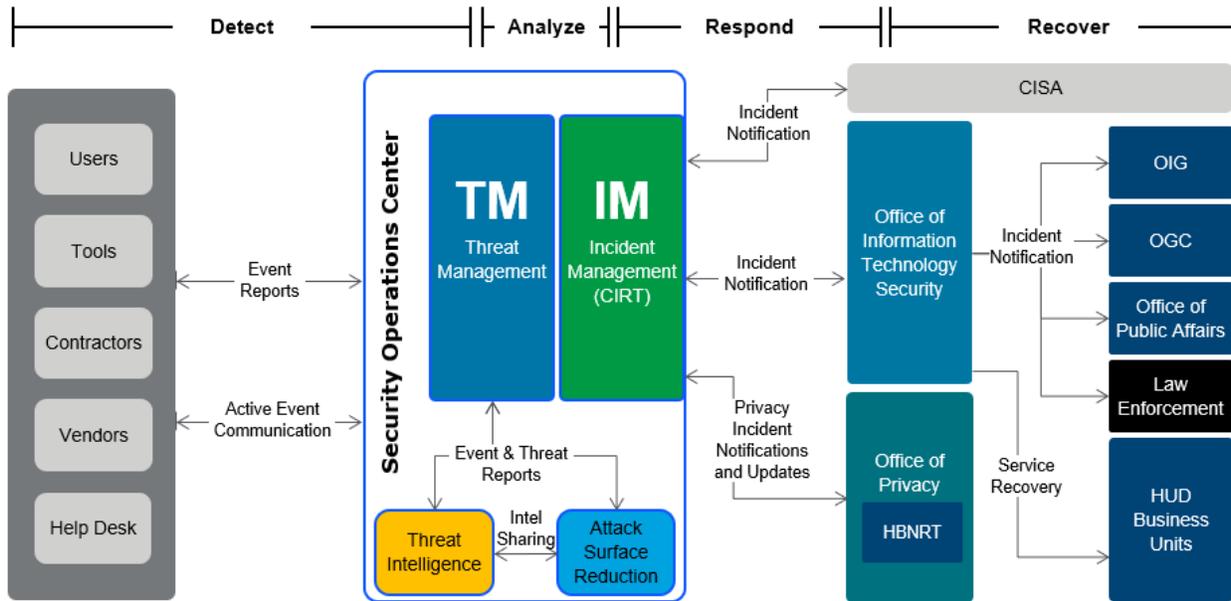


Figure 2: Communication Flow

HUD CIRT utilizes a central ticketing system as the primary method of incident documentation and coordination. HUD CIRT and the broader HUD SOC shall receive event and incident information through phone, email, and in person. The contact information of stakeholders identified with responsibilities in managing, handling, or responding to cybersecurity incidents are listed in Appendix B of this document.

The CISO will designate an Incident Commander for all major incidents defined in Section 3.3 and ensure they have all the resources needed to remediate incidents in an effective and efficient manner. For non-major incidents, the IM Lead will serve as the Incident Commander. When applicable, the IM Lead will notify the HBNRT of any incidents that involve the exposure, or potential exposure, of Personally Identifiable Information (PII) / Sensitive Personally Identifiable Information (SPII).

If an incident indicates that federal or civil laws may have been violated, the Incident commander or IM Lead will refer the incident to the HUD Director of the Physical Security Division, Headquarters Office of Security and Emergency Planning.



3. Incident Taxonomy and Data Flow

This section will describe incident taxonomy which will allow the IM team to track incidents and their characteristics over time, providing valuable security operations data for both internal use and regular reporting purposes.

3.1 Incident Definition

A **cybersecurity incident** as defined by NIST 800-53 Revision 4 is any occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or, constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

HUD CIRT works to contain and remediate incidents in a timely and effective manner through the analysis of cybersecurity alerts. An alert is an indicator of malicious activity based on the aggregation, correlation, and/or analysis of events; an event is any observable occurrence in a system or network. Alerts may comprise system- or application-generated notifications (e.g., antivirus alerts), user-reported indicators of suspicious activity, single-instance anomalies, or any other indicator of malicious behavior.

3.2 Incident Data Flow

Incidents generally begin as events or alerts captured either by HUD's suite of cyber tools (e.g. Security Incident and Event Management (SIEM), endpoint antivirus, intrusion protection/detection systems), phone calls to the SOC, emails to the SOC email distribution, IT vendors, or from CTI reports.

The TM team serves as the initial point of contact for ingesting, detecting, and analyzing events and alerts to determine if they meet the criteria for an incident.

When events/alerts meet incident criteria, the TM team will open an incident ticket(s) with an initial assessment of the nature of the incident that will then be passed on to HUD IM/CIRT to manage IR. Details concerning the IR process can be found in Section 4 of this document.

3.3 Incident Data Elements to Record

The SOC will continually capture data points throughout the incident lifecycle to satisfy reporting requirements and to drive continuous improvement of security operations. Appendix C of this document maps out at what stage incident data elements should be recorded by various SOC analysts.



Cybersecurity Incident Response Plan

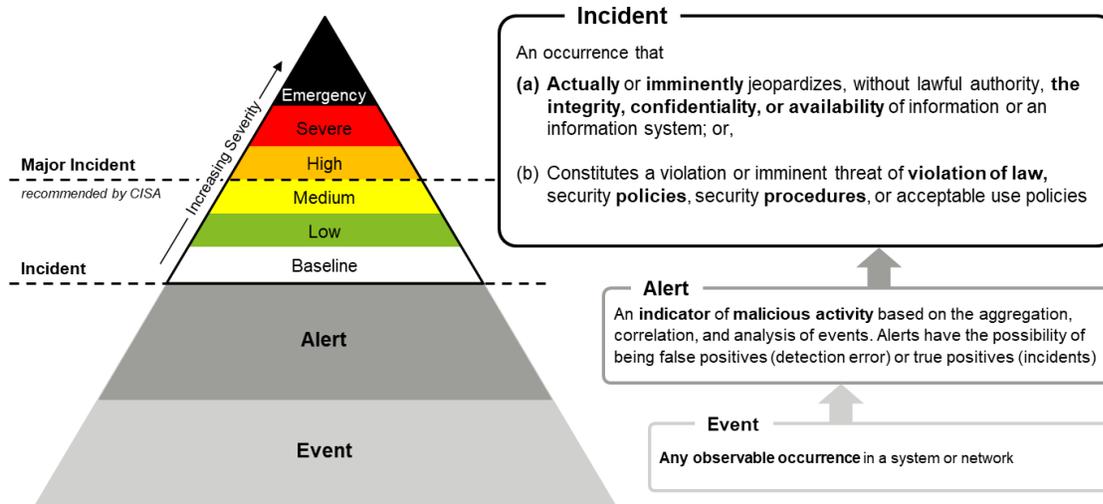


Figure 3: Incident Types

Incident Categorization and Scoring

A **Major Incident**, as defined by OMB M-17-05, is any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. HUD is responsible for determining if an incident should be designated as major but may consult with CISA to make that determination. If an incident rises to the level of High (Orange), CISA will require that HUD designate it as major.

A **Privacy Incident** as defined by the HUD Breach Notification Policy and Response Plan is 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. 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 of 2015.

The overall severity ranking of an incident is commonly used to summarize the incident’s impact, scope, urgency, and necessary level of response. HUD adopts the National Cybersecurity and Communications Integration Center (NCCIC) Cyber Incident Scoring System (NCISS) severity schema in order to align internal severity levels with those utilized by CISA and other Federal Departments and Agencies. See Figure 4 for NCCIC NCISS severity schema definitions.



Cybersecurity Incident Response Plan

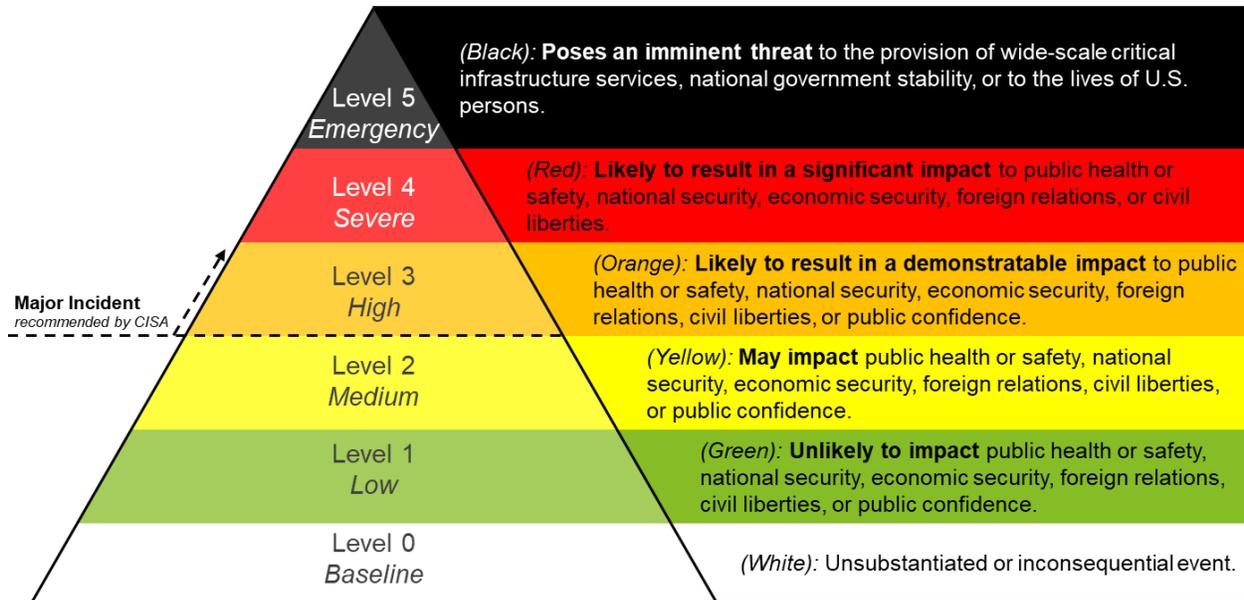


Figure 4: NCISS Incident Severity Levels (reference Cybersecurity Infrastructure Security Agency)

To calculate an incident’s severity, HUD CIRT will add the functional, informational, recoverability and location of observed activity impact scores together (see Figure 5).

Level 0 Baseline (White)	0 – 9
Level 1 Low (Green)	10 -15
Level 2 Medium (Yellow)	16 – 21
Level 3 High (Orange)	22 – 27
Level 4 Severe (Red)	28 - 29
Level 5 Emergency (Black)	30

Figure 5: Incident Severity Scoring



1. Functional Impact: Functional impact is a measure of the actual, ongoing impact to the organization. In many cases (e.g., scans and probes or a successfully defended attack), minimal or no impact may be experienced due to the incident (see Table 1).

Severity Level	Description	Points
NO IMPACT	Event has no impact.	0
NO IMPACT TO SERVICES	Event has no impact to any business or Industrial Control Systems services or delivery to entity customers	2
MINIMAL IMPACT TO NON-CRITICAL SERVICES	Some small level of impact to non-critical systems and services	3
MINIMAL IMPACT TO CRITICAL SERVICES	Minimal impact but to a critical system or service, such as email or Active Directory	4



Cybersecurity Incident Response Plan

SIGNIFICANT IMPACT TO NON-CRITICAL SERVICES	A non-critical service or system has a significant impact	6
DENIAL OF NON-CRITICAL SERVICES	A non-critical system is denied or destroyed	7
SIGNIFICANT IMPACT TO CRITICAL SERVICES	A critical system has a significant impact, such as local administrative account compromise	9
DENIAL OF CRITICAL SERVICES/LOSS OF CONTROL	A critical system has been rendered unavailable	10

Table 1: Functional Impact Scoring and Definitions (Reference CISA Federal Incident Notification Guidelines)

2. Information Impact: In addition to functional impact, incidents may also affect the confidentiality and integrity of the information stored or processed by various systems. The information impact category is used to describe the type of information or data lost, compromised, or corrupted (see Table 2).

Severity Level	Description	Points
NO IMPACT	No known data impact	0
SUSPECTED BUT NOT IDENTIFIED	A data loss or impact to availability is suspected, but no direct confirmation exists.	1
PRIVACY DATA BREACH	The confidentiality of PII or personal health information (PHI) was compromised	2
PROPRIETARY INFORMATION BREACH	The confidentiality of unclassified proprietary information, such as protected critical infrastructure information, intellectual property, or trade secrets was compromised	5
DESTRUCTION OF NON-CRITICAL SYSTEMS	Destructive techniques, such as master boot record (MBR) overwrite; have been used against a non-critical system	6
CRITICAL SYSTEMS DATA BREACH	Data pertaining to a critical system has been exfiltrated	7
CORE CREDENTIAL COMPROMISE	Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated	8
DESTRUCTION OF CRITICAL SYSTEM	Destructive techniques, such as MBR overwrite; have been used against a critical system	10

Table 2: Information Impact Scoring and Definitions (Reference CISA Federal Incident Notification Guidelines)

3. Recoverability: Recoverability represents the scope of resources needed to recover from an incident. In many cases, HUD’s internal computer network defense staff will be able to handle an incident without external support, resulting in a recoverability classification of Regular. In Extended recoverability cases, significant efforts such as a multi-agency, multi-organizational response task force may be needed for recovery. Lastly, it may not be feasible to recover from some types of incidents, such as significant confidentiality or privacy compromises (see Table 3).



Cybersecurity Incident Response Plan

Severity Level	Description	Points
REGULAR	Time to recovery is predictable with existing resources	2
SUPPLEMENTED	Time to recovery is predictable with additional resources	4
EXTENDED	Time to recovery is unpredictable; additional resources and outside help are needed	6
NOT RECOVERABLE	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly)	10

Table 3: Recoverability Impact Scoring and Definitions (Reference CISA Federal Incident Notification Guidelines)

4. Location of Observed Activity: The logical location of observed malicious activity within the network environment (see Table 4).

Location	Description	Points
LEVEL 1 – BUSINESS DEMILITERIZED ZONE	Activity was observed in the business network’s demilitarized zone (DMZ)	2
LEVEL 2 – BUSINESS NETWORK	Activity was observed in the business or corporate network of the victim. These systems would be corporate user workstations, application servers, and other non-core management systems	4
UNKNOWN	Activity was observed, but the network segment could not be identified	5
LEVEL 3 – BUSINESS NETWORK MANAGEMENT	Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores	6
LEVEL 4 – CRITICAL SYSTEM DMZ	Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay “jump” boxes into more critical systems	7
LEVEL 5 – CRITICAL SYSTEM MANAGEMENT	Activity was observed in high-level critical systems management such as human-machine interfaces in industrial control systems	8
LEVEL 6 – CRITICAL SYSTEMS	Activity was observed in the critical systems that operate critical processes, such as programmable logic controllers in industrial control system environments	9
LEVEL 7 – SAFETY SYSTEMS	Activity was observed in critical safety systems that ensure the safe operation of an environment. One example of a critical safety system is a fire suppression system	10

Table 4: Location of Observed Activity Impact Scoring and Definitions (Reference CISA Federal Incident Notification Guidelines)

Additional Essential Incident Data Elements

HUD CIRT and TM analysts will collect and track other pertinent information necessary for the investigation, containment, and remediation of cybersecurity incidents in addition to the four data elements used to calculate incident severity described earlier. In some cases, it may not be feasible to have complete and validated information when filing out the incident details. HUD CIRT and TM analysts will fill out the incident ticket based on obtainable data and update the ticket as more complete information becomes available.

The below list of incident characteristics is not exhaustive but provides a sampling of the various types of incident data the HUD SOC will collect and track throughout the normal IR process. Appendix C provides guidance on when these metrics can be captured during the IM lifecycle.



Cybersecurity Incident Response Plan

Attack Vectors: Avenues by which a threat actor jeopardizes the integrity, confidentiality, or availability of information or an information system. CISA incident notification guidelines require that all incident reports include one of the following nine attack vector categories. See Table 5 for descriptions and definitions concerning attack vectors.

Attack Vector	Description	Example
UNKNOWN	Cause of attack is unidentified	This option is acceptable if cause (vector) is unknown upon initial report. The attack vector will be updated in a follow-up report
ATTRITION	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services	Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures
WEB	An attack executed from a website or web-based application	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware
EMAIL / PHISHING	An attack executed via an email message or attachment	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message
EXTERNAL / REMOVABLE MEDIA	An attack executed from removable media or a peripheral device	Malicious code spreading onto a system from an infected flash drive
IMPERSONATION / SPOOFING	An attack involving replacement of legitimate content/services with a malicious substitute	Spoofing, man in the middle attacks, rogue wireless access points, and structured query language injection attacks all involve impersonation
IMPROPER USAGE	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system
LOSS OR THEFT OF EQUIPMENT	The loss or theft of a computing device or media used by the organization	A misplaced laptop or mobile device
OTHER	An attack method does not fit into any other vector	

Table 5: Attack Vector Taxonomy (Reference CISA Federal Incident Notification Guidelines)

Threat Matrix: Tool used to classify the type of threat actor behind any particular incident. Threats may be rated as Internal/Indirect, Internal/Direct, External/Indirect, or External/Direct. Understanding threat attribution will help HUD determine risk areas and how HUD is being targeted by malicious actor(s). See Figure 6 on how threats will be classified.



Cybersecurity Incident Response Plan

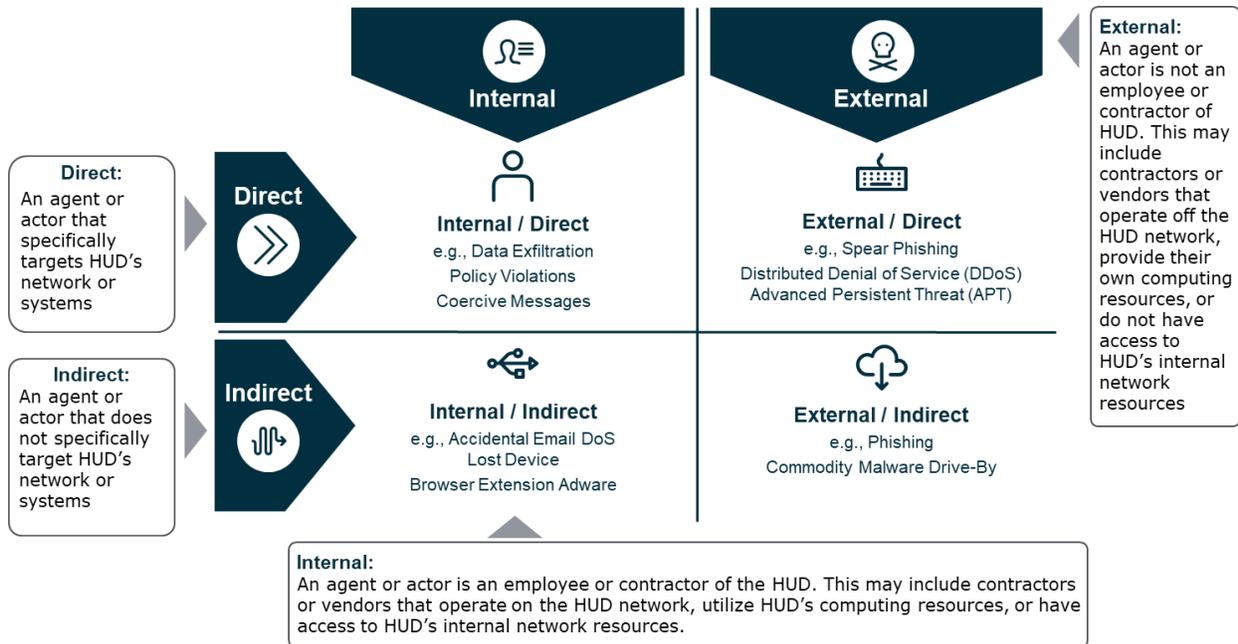


Figure 6: Threat Matrix basic attribution model

Indicators of Compromise (IOCs): Any observable occurrence or computer artifact that indicates an information system may be compromised. While indicators are used regularly in day-to-day IM activities, the long-term preservation of IOCs for both major and minor incidents provide valuable intelligence that can be used to correlate incidents previously thought to be unrelated. IOCs may include:

- Malicious Uniform Resource Locators (URLs), Internet Protocols (IPs), domains
- Phishing email (sender/receiver addresses, subject line)
- File hashes
- Anomalous traffic indicating data exfiltration to unknown or malicious destinations
- File paths (with or without wildcards) registry keys, and more

Appendix D of this document provides a checklist of sources to investigate incidents for indicators of compromise.

3.4 Sensitive Data

The IM function will ensure that CIRT minimizes the likelihood of disclosure and sharing of sensitive HUD data if sensitive data is encountered during the course of an incident investigation. All SOC personnel will practice specialized handling and response protocols when HUD sensitive data may be involved to ensure minimal impact to public safety, national and economic security, foreign relations, civil liberties, or public confidence. Two specialized subsets of data the SOC recognizes are **PII** and **SPII**. The definitions of each data type and their relationship are listed below in Table 6.



Cybersecurity Incident Response Plan

Data	Definition
PII	Information which can be used to distinguish or trace an individual's identity, either by itself or when combined with other information which is linked or linkable to a specific individual. PII demands a case-by-case assessment of the specific risk that an individual can be identified, with recognition 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.
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, account numbers, and any other unique identifying number (e.g., Federal Housing Administration case number, driver's license number, or financial account number, etc.). Other data elements such as citizenship or immigration status; medical information; ethnicities, religious affiliations, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also SPII.

Table 6: Sensitive Data Definitions (Reference DHS Privacy Office Handbook for Safeguarding Sensitive PII)

4. Incident Response Framework

IR is defined as the summary of technical activities performed to prepare, detect, analyze, respond, recover, and review cyber incidents. **Incident handling** is defined as the summary of processes and predefined procedural actions to handle/manage an incident effectively and actionably. This IR framework provides a defined, repeatable, and measurable process by which HUD can effectively respond and handle cybersecurity incidents.

HUD's IM function follows an organized approach to incident handling, providing situational awareness to SOC stakeholders via established reporting mechanisms and coordinating incident preparation, recovery, and review actions across IT functions. HUD's IR function validates suspected incidents to direct response and recovery activities from confirmed incidents.

This IR framework is structured in six-phases derived from NIST Special Publication 800-61r2. It is designed to drive efficient IR and handling processes among all SOC personnel, and to support consistent incident tracking and reporting (Figure 7).

HUD's IR framework comprises the following phases:

1. Prepare

Ensures that HUD is equipped with the processes, technologies, and personnel necessary to effectively and efficiently respond to alerts, in addition to the ASR team continually verifying that the proper safeguards are established to minimize the risk of an incident occurrence

2. Detect

Establishes and configures the technologies and processes to enable the timely and accurate ingestion, aggregation, and correlation of events from technical and non-technical sources across the environment with credible intelligence in order to generate and deliver security alerts to CIRT personnel



Cybersecurity Incident Response Plan

- 3. Analyze**
Investigates and analyzes security alert(s) in order to determine whether an incident has occurred
- 4. Respond**
Contains and mitigates the threat of confirmed incident
- 5. Recover**
Eradicates threats from the environment and restores all systems to normal business operations after an incident has been fully contained
- 6. Review**
Evaluates previous incidents, both individually and in aggregate, to determine how to better respond to further incidents and to protect the environment from their occurrence

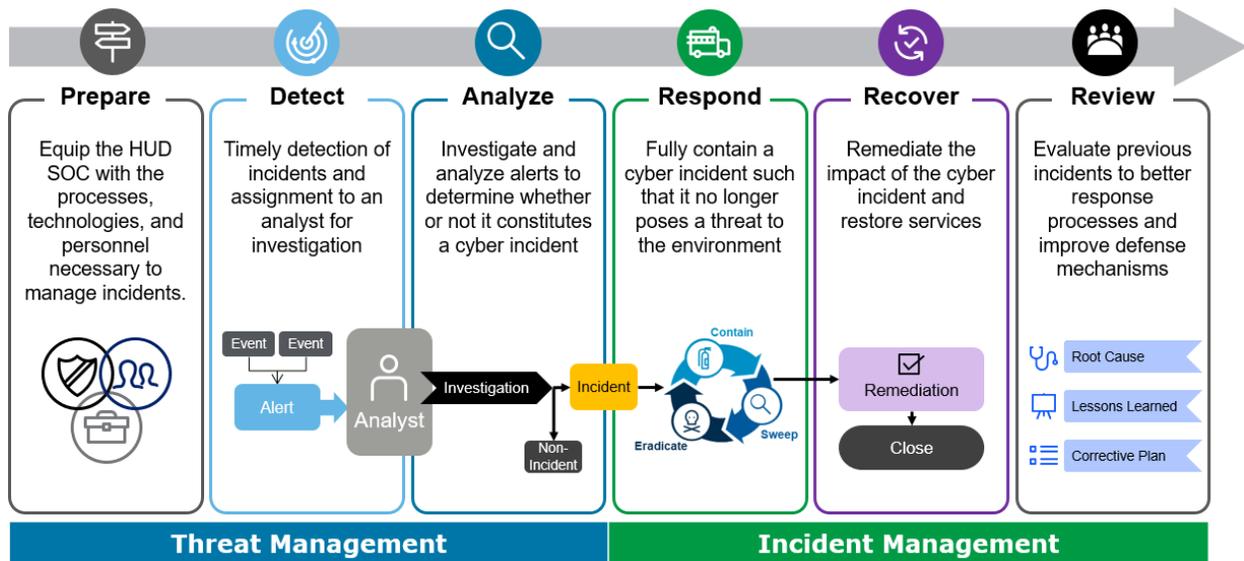


Figure 7: IR Framework

The matrix in Table 7 below defines responsibility, accountability, consultation, and SOC functions informed during each phase of the IR Framework.

	Threat Management	Incident Management	Threat Intelligence	Attack Surface Reduction
Prepare	R	R	R	R
Detect	R, A	C	C	C
Analyze	R, A	C, I	C	C
Response	C, I	R, A	C	C
Recover	C, I	R, A, C	I	C, I
Review	C, I	R, A	C, I	C, I

Table 7: IR RACI



Cybersecurity Incident Response Plan

Key:

(R) Responsible: Responsible for completing tasks during a give phase in the IM framework

(A) Accountable: Ultimately answerable for the correct completion for a given phase

(C) Consulted: Provides subject matter expertise or recommends specific courses of actions to take place during a given phase

(I) Informed: Kept up to date on a given phase in the IM framework

4.1 Prepare



The objective of the Prepare phase is to create the necessary conditions and prerequisites for HUD CIRT to respond to cybersecurity incidents as well as aid effectively and efficiently in protecting the environment against future incidents. This phase is an operational process that all major processes of the SOC continuously complete in partnership with HUD IT stakeholders. In pursuit of this goal the following actions shall take place from a Technology, Process, and Personnel perspective:

Technologies

- HUD shall use a ticketing system for tracking incident information and status. The ticketing system is used in the incident tracking processes by the IM members, IT Service Providers, Privacy Office, OITS, and IOO. This platform allows for comprehensive record keeping throughout the IR process, from detection through recovery and review, to ensure critical observations and technical details are captured to support later evidentiary or technical analysis needs
- HUD shall employ a variety of detection and prevention mechanisms throughout the HUD IT environment to monitor network traffic and device activity. Tools collecting HUD cyber data include anti-malware agents, Data Loss Prevention (DLP), endpoint detection & response, firewalls, and intrusion detection and prevention systems. IT service providers and HUD CIRT members shall review and respond to alerts generated by these technologies either through a dashboard of a specific cybersecurity tool or from the SOC's SIEM platform. See Appendix E for a list of current technologies used by the SOC
- HUD shall employ extensive network and endpoint event logging to correlate and detect suspicious activity from disparate sensors across the environment. Event logs are centrally stored for usage by IT service providers and IM personnel. The SOC's SIEM platform is utilized to analyze these logs
- HUD SOC team shall maintain the SIEM platform. The SOC will update, modify, or create use cases to alert against possible cybersecurity incidents occurring throughout HUD's network enterprise



Cybersecurity Incident Response Plan

- HUD SOC shall save incident artifacts securely to support investigations as needed
- HUD shall ensure updates for malicious code protection mechanisms are applied whenever new releases are available in accordance with organizational configuration management policy and procedures
- Restrict users' permissions to install and run software applications and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network
- Use application whitelisting to allow only approved programs to run on a network
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users
- Configure firewalls to block access to known malicious IP addresses
- If HUD lacks any of the above capabilities or technologies in-house, HUD shall augment their capabilities through external technology and service contracts as needed

Processes

- HUD shall have 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
- The IR Plan, to include this IR Plan, shall be reviewed and tested against federal standards and HUD policy to ensure the effectiveness of HUD's IR capability
- HUD SOC shall coordinate with IT service providers and other HUD cybersecurity teams to review, maintain, and consult on existing or new processes and technologies that serve to prevent and detect cyber incidents
- HUD CIRT shall review cyber trends, TI, lessons learned and incident tickets from past incidents to proactively prepare for new and emerging threats.
- If at any point during an investigation it is discovered that there could be a privacy impact, execute the PII notification and reporting procedure

Personnel

- HUD CIRT will maintain contact information for all members of the IR process
- HUD CIRT personnel will be available 24/7. When not on site, HUD CIRT personnel will be on-call in the event of a major incident
- The SOC Director shall ensure HUD SOC personnel are trained and prepared to identify, report, and respond to potential incidents
- The SOC Director or appointed leads shall verify that HUD's IT vendors adhere to contractual agreements with reporting and response requirements relating to cybersecurity incidents
- HUD CIRT shall prepare for incidents by building and maintaining any incident-related skills and by facilitating communication and coordination throughout the organization
- All HUD employees and contractors shall be trained on how to identify and report malware incidents to HUD CIRT via email at cirt@hud.gov, by phone to the help desk at



Cybersecurity Incident Response Plan

(202-708-3300), or by simply entering a Service Desk ticket at <http://servicedesk.hud.gov>

Maintain Record Keeping and Central Management of Knowledge

- The SOC Director, with assistance of the SOC team will retain all investigation and incident information in a central repository for at least one year, including all required data points per the established taxonomy in addition to other characteristics, such as:
 - Incident risks
 - Threat actor characteristics
 - Attack vectors or patterns
 - Observations / IOCs (e.g. IPs, URLs, domains, file name, hashes, mutexes, email subject, etc.)
 - Process notes and milestones
- The SOC must maintain comprehensive record keeping throughout the IR process, from detection through recovery and review, to ensure critical observations and technical details are captured to support later evidentiary or technical analysis needs

4.2 Detect



The objective of the Detect phase is to detect cyber events and incidents in a timely manner to reduce the time from an attacker's initial entry to the time the intrusion is detected -- known as 'dwell time.' Decreasing dwell time will reduce the amount of time that attackers can access HUD networks, the potential amount of data lost, the operational impact, and the regulatory penalties of such incidents.

This phase shall be carried out by TM analysts in the SOC with support and input from CIRT.

HUD will leverage both technical and non-technical sensors to gather telemetry data from its environment in order to detect and alert on suspicious activity. Technical sensors include any internet-capable devices such as user endpoints, mobile devices, security appliances, network devices, and applications, such as antivirus agents, DLP agents, or web applications. These technical sensors analyze events and automatically generate alerts when rulesets are triggered (e.g. identification of malware, suspected data loss event).

Technical sensor data will then be forwarded to the SOC's SIEM platform for the SOC to analyze. The SIEM will be managed by a SIEM engineer. The SIEM engineer shall develop use cases to correlate events that will trigger alerts inside the SIEM for TM analysts to investigate and analyze. The SIEM engineer will collaborate with the entire SOC, specifically the TI and TM teams to continuously tune use cases to minimize the false positive ratio.

To determine their applicability and effectiveness, monthly review of use cases should be scheduled. The SIEM engineer, with input from other members of the SOC team, will work to



Cybersecurity Incident Response Plan

retire obsolete use cases, update existing rules, and create additional use cases that will identify new and emerging threats based on TI.

Non-Technical sensors include any person or process actively or passively monitoring the environment for suspicious activity. Non-Technical data is not collected by a SIEM but can be useful in the incident report with proper documentation. The IM team will work with other groups within HUD to ensure that the business and users are aware of the means by which they can report cyber security incidents and that those reports are received in a timely manner. Examples of non-technical sensor include emails to the HUD SOC email distribution, phone calls to the Help Desk, face-to-face communications, and TI reports. Refer to Figure 8 to see an illustration of the steps to be taken in the process of detecting an incident.

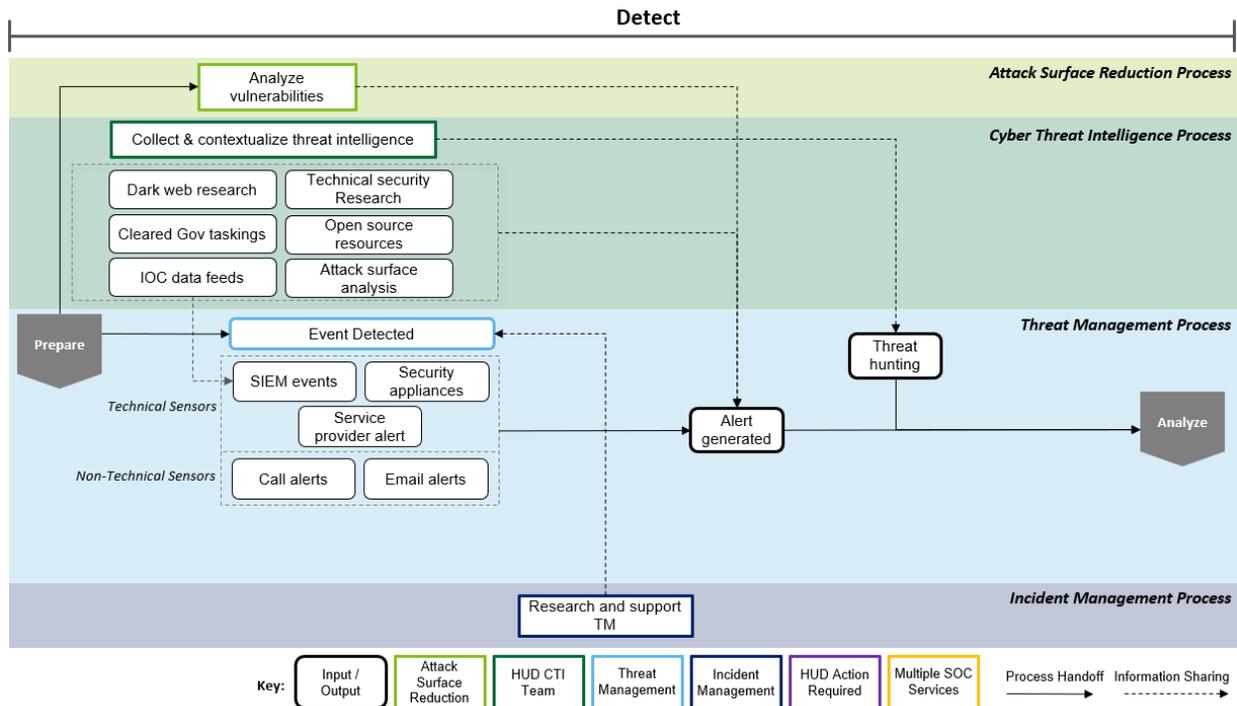


Figure 8: Detect Phase Workflow

4.3 Analyze



The objective of the Analyze phase is to quickly and accurately investigate and triage incident alerts and reports to determine their validity with the end goal to provide a preliminary assessment of an incident's impact, if valid. Having a wealth of information about a valid incident allows for proper containment, remediation, and recovery decisions. This phase is largely carried out by TM analysts in the SOC, but it is done with the support and input from CIRT.



Cybersecurity Incident Response Plan

HUD has established a log retention policy of at least one year in the HUD IT Security Handbook 2400.35 Rev 5. When a security concern is raised or detected, the TM analyst reviews the alerts to validate that an incident has occurred, assess the scope, determines the attack vector, and fills out the incident ticket with as much detail as possible. Once the incident has been escalated, HUD CIRT may request additional logs from contractors and program offices to further investigate incidents that are already being tracked by HUD CIRT.

HUD CIRT then correlates logs from different sources to create an accurate timeline of the incident. Reference Appendix D for a checklist of logs that should be collected for incident investigation HUD CIRT.

Log data collected as seen in Appendix D shall assist the TM analyst and CIRT in characterizing the nature of the incident and the potential threat and impact to HUD. Collected log data should allow for analysis related to:

- Deviation from normal behaviors of networks, systems, applications, and users. Based on pre-establish profiles of behaviors or policies, outliers may provide indicators of how an incident affects HUD systems
- Correlation between incident behavior and IOCs against TI and network traffic to identify time, location, and affected users/systems of an incident or incidents
- Correlation between incident behavior and past incidents to check for recurring threats

HUD CIRT will document information they have gathered to assist in future post-incident analysis and lessons learned. Some examples of data to document include:

- 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

HUD CIRT may also contact CISA when necessary to request assistance with analysis. HUD has a Federal Network Authorization on file with CISA. This authorization allows the CISA Digital Analytics Branch and CIRT, to mobilize to HUD promptly to aid with major incidents. Refer to Figure 9 to see an illustration of the steps to be taken in the process of analyzing an incident.



Cybersecurity Incident Response Plan

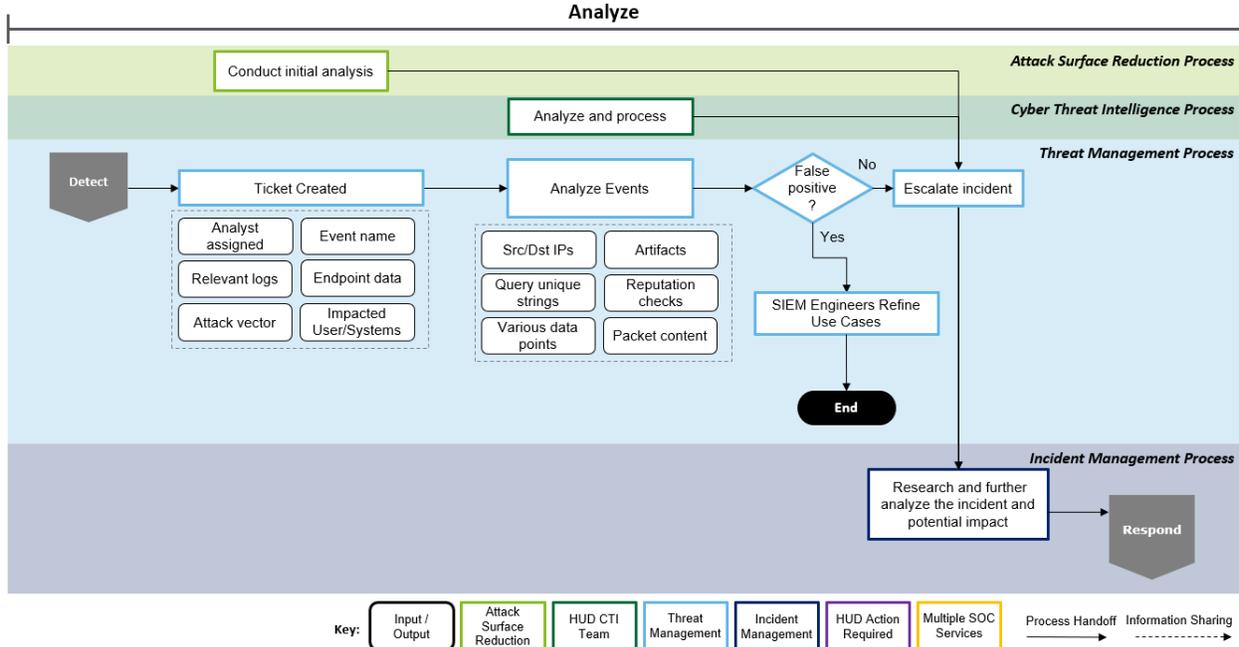


Figure 9: Analyze Phase Workflow

4.4 Respond



The objective of the Respond phase is to contain a cybersecurity incident in such way that the threat actor(s) do no longer pose an actual or imminent threat to HUD’s environment and to communicate the incident to internal and external stakeholders, including leadership, users, program offices, contractors, and vendors.

Communication

HUD CIRT will communicate incidents to appropriate individual users, system owners, and HUD OITS leadership. HUD CIRT will validate the incident’s scope, severity, and impact in accordance with applicable regulatory requirements as accurately as possible as new incident information becomes available and notify stakeholders of any substantive changes. HUD CIRT will also adhere to CISA and Congress reporting requirements defined in Section 5.

If the incident occurs at/by a third party, HUD CIRT will advise the system owner and/or HUD business lead if a legal contract and business associate agreement exist. It is incumbent on the affected system owner and/or business lead to work with the Legal Department and the department holding the contract/business associate agreement to review the contract terms and determine the next course of action to remediate an incident that affects HUD infrastructure or data.



Cybersecurity Incident Response Plan

In the event an incident is classified as a potential breach, the CIRT team will contact HBNRT immediately to provide the incident number and any other pertinent details. Additionally, CIRT analysts will contact the privacy office to inform them of the potential breach. CIRT should continue to contact the privacy office until the incident is acknowledged.

Contain, Sweep, Eradicate

The CIRT and applicable members of the SOC team will work with IOO, system owners and other appropriate HUD stakeholders to contain, sweep, and eradicate incidents.

Containment involves isolating threats so that they do not spread, infect, or otherwise negatively impact other areas of the HUD network. A general list of steps that CIRT can assist HUD system owners and stakeholders to complete include:

- Use information from the detect and analyze phases to identify any vulnerabilities exploited
- Identify and isolate affected endpoints from network, apply patches if available
- Block IPs, Domains, Email Senders
- Disable / Reset user accounts
- Other containment actions to isolate or disable accounts, devices, applications, and systems

Sweeping involves enumerating the spread of an incident and identifying additional associated threats on the HUD network. Sweeping involves reviewing the SIEM and other sources of cybersecurity alerts such as anti-virus and other logs listed in Appendix D. General list of sweep activities include:

- Analyzing exploited threats for indicators
- Scan network for matching indicators
- Scan endpoints for matching indicators
- Use network and endpoint scan results to correlate additional compromise
- Collect and analyze artifacts for any matches for additional indicators
- If sweeping activities identify additional areas of incident indicators, repeat the containment step

CIRT will coordinate sweep activities with the SOC ASR analysts and the HUD Continuous Diagnostics and Monitoring (CDM) team. The CDM team will conduct network scans while SOC ASR team will analyze specific vulnerabilities that may have caused the incident. Additionally, CIRT will contact system owners and other HUD stakeholders as necessary to assist the CIRT in enumerating the extent of an incident and provide consult in containing incident threats. HUD CIRT will also coordinate with the Vulnerability Management team in remediating vulnerabilities that may have been exploited.

HUD CIRT shall partner with HUD system owners and affected stakeholders to repeat contain and sweep activities until all incident related threats are discovered. Incident eradication entails removing the threat and restoring affected systems to their previous state, ideally while minimizing data loss.



Cybersecurity Incident Response Plan

At the end of the Respond phase, CIRT and other major functions of the HUD SOC should retain evidence or documentation of affected users, endpoints, systems, data, and applications. They must also annotate the times on the incident ticket when the sweep and containment activities started and completed for metrics and reporting purposes. Refer to Figure 10 to see an illustration of the steps to be taken in the process of responding to an incident.

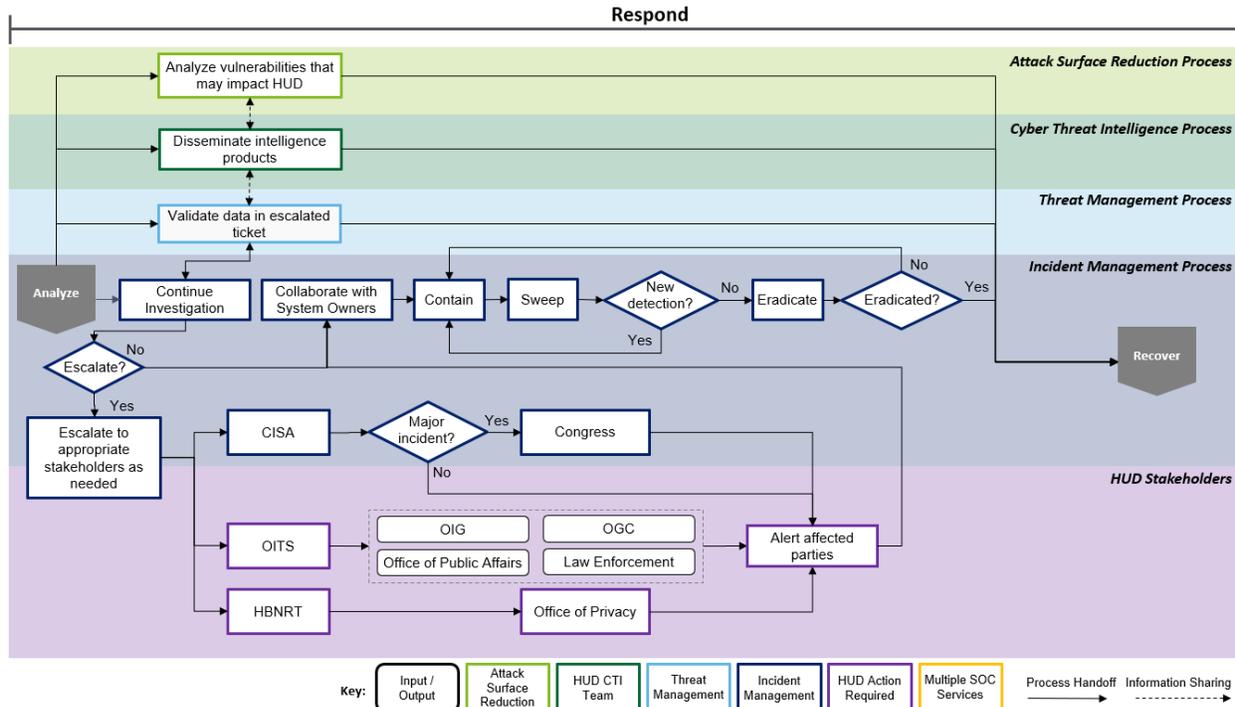


Figure 10: Respond Phase Workflow

4.5 Recover



The objective of the Recover phase is to restore systems to normal operation, confirm that the systems function normally, and (if applicable) remediate other potential vulnerabilities to prevent similar incidents. System owners and administrators will be the responsible personnel for completing removing. The Cyber TI Team will continue to gather Intel to provide to HUD CIRT in the event that the threat has a new attack vector or IOCs. The TM team will assist recovery and restoration efforts by providing information on how an incident may have affected systems as well as recommendations on restoring services.

The HUD CIRT team supports remediation activities, working with IT, system owners, and vendors to ensure that any damages have been rectified. Activities include reimaging and rebuilding affected devices, restoring data to affected systems (if applicable), hardening access controls, reconfiguring firewall rules, reinitializing applications, or other incident remediation activities that will defend the network and services against future similar incidents.



Cybersecurity Incident Response Plan

Additionally, when restoring services, systems or data, the team should consider the attack vector, the affected data, and the timeline in which the attack initially took place -- which should have been discovered and documented as part of the Analyze phase. This step in the recovery process is critical to preventing the re-introduction of vulnerabilities, malware, and corrupted data into the operating environment. Refer to Figure 11 to see an illustration of the steps to be taken in the process of recovering from an incident.

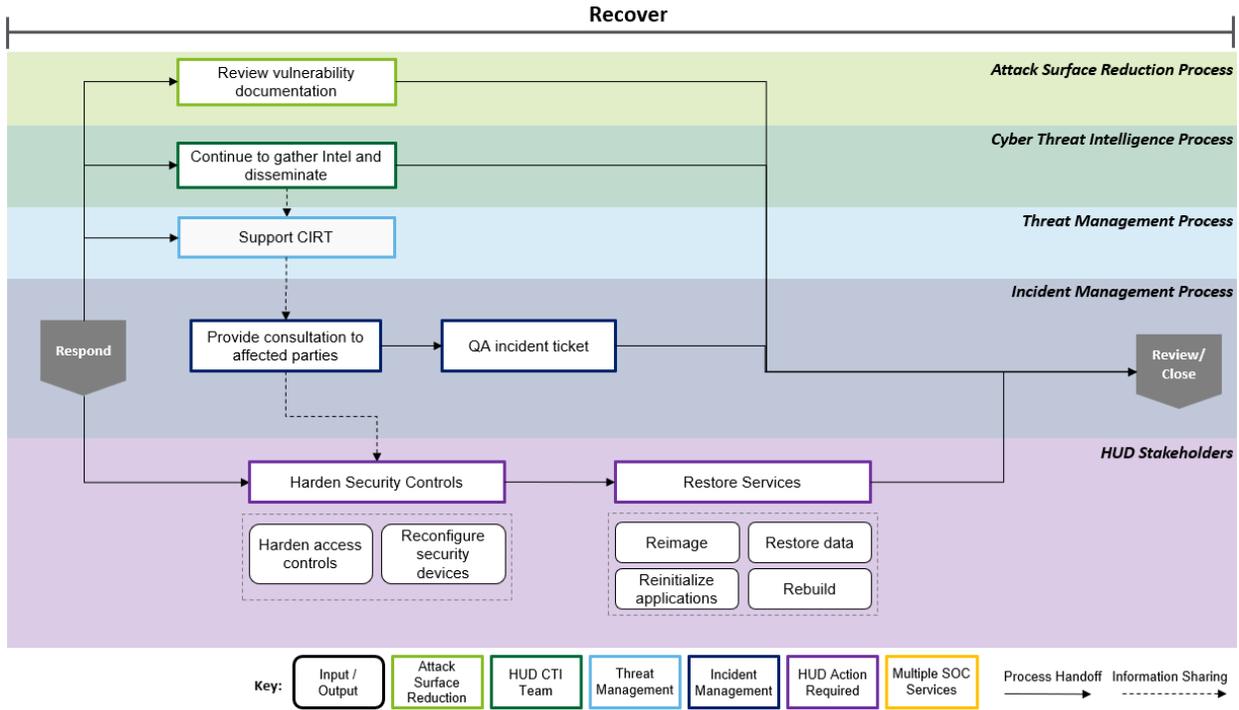


Figure 11: Recover Phase Workflow

4.6 Review



The objective of the Review phase is to assess how effectively the IR Plan was executed and identify deficiencies, and possible improvements. This phase involves all HUD SOC and affected stakeholders, as applicable.

HUD IM notifies stakeholders of the completion of the recovery phase and can begin to review the ticket for closure when affected services, systems or data are properly restored and documentation is complete. Incidents can only be closed once the final post-incident analysis report is complete. Incidents can only be closed by the incident commander for major incidents, or by the IR lead for non-major incidents. A template for a post-incident analysis report can be found in Appendix F.



Cybersecurity Incident Response Plan

Within **seven (7) calendar days** of closing incidents, the IM team should hold a “lessons learned review” with the involved stakeholders to note lessons learned and identify future areas of improvement. Appendix G provides a template needed to complete Lessons Learned. Non-major incidents should be reviewed at routine team meetings as needed. Example prompts and questions the team may use for lessons learned includes:

- Exactly what happened, and at what times?
- Who was involved? What particular business units?
- What was the root cause of the incident?
- Were the documented processes followed correctly?
- How effective was each of the five (5) previous phases: Prepare, Detect, Analyze, Respond, and Recover? Were there any notable issues in one or more of the phases?
- Were any resources or information unavailable, or difficult to obtain?
- What processes or technology could have prevented or mitigated this incident? This could be either for CIRT itself, or for the system or program office that was impacted.
- What tools or resources are needed to detect, analyze, and mitigate future incidents, if any?

The review phase will result in a documentation that will be used to: provide funding justification, provide long term technology recommendations, refresh intelligence requirements, provide artifacts to include in risk assessments, and create metrics to assess IM/IR effectiveness (e.g. communication, dwell time, manpower per incident, cost per incident, etc.).

In accordance with General Records Schedule 24, section 3.4.2, HUD will retain incident handling records for three years. If incident handling records are part of a criminal investigation, they must be retained until all legal actions have been completed. Refer to Figure 12 to see an illustration of the steps to be taken in the process of reviewing an incident.

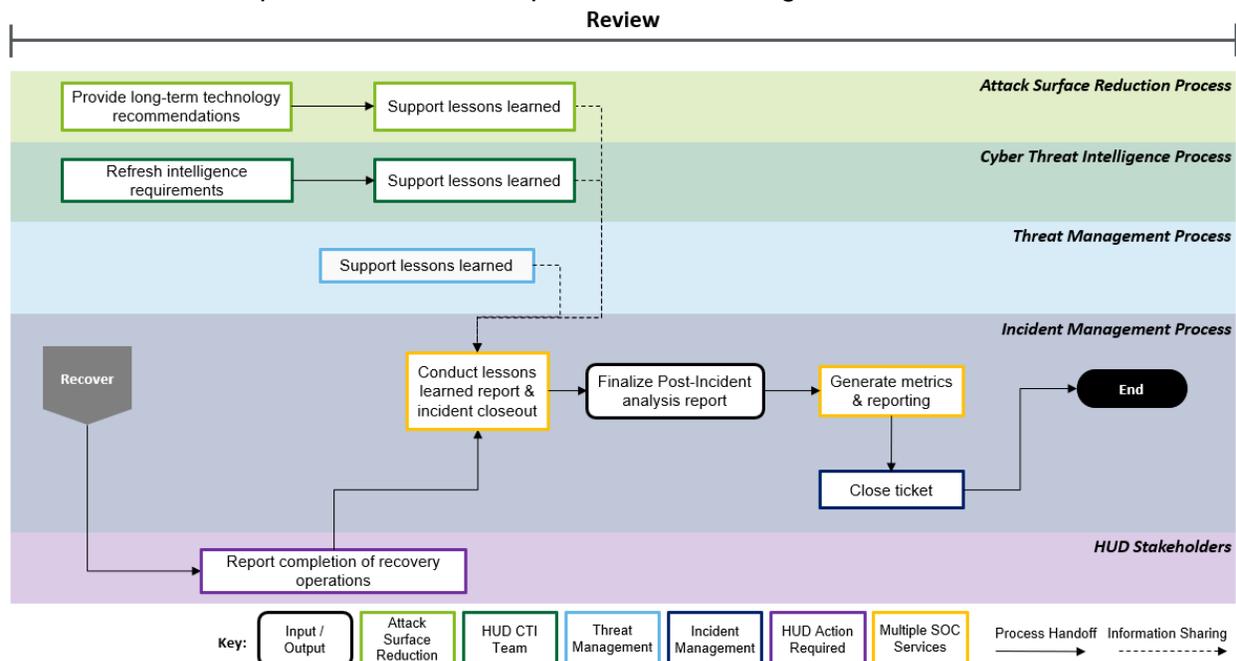


Figure 12: Review Phase Workflow



5. Incident Reporting Requirements and Metrics Maintenance

HUD shall submit incident reports in accordance with CISA, FISMA, and Congressional requirements. HUD will produce an annual FISMA report to include cybersecurity incident information and quarterly reports to meet OMB requirements. Outside of the annual and quarterly reports, HUD is responsible for reporting certain incidents to CISA and Congress for major incidents or upon request.

HUD SOC will collect variables data to assess metrics at each phase of the IR framework as depicted in Figure 13. The detailed dataset that shall be captured can be found in Appendix C. The SOC team will continuously capture and analyze data against defined metrics through ticket information, reports from HUD’s SIEM solution, and other cybersecurity tools as needed to keep HUD leadership aware of cybersecurity incidents and their impact to HUD. The IM function will also note response times when incident data is shared with internal and external stakeholders (e.g. CISA). Key metrics that the SOC will maintain include:

- Time to detect
- Time to report
- Time to create
- Time to acknowledge
- Time to notify
- Time to validate
- Time to respond
- Time to contain
- Time to remediate
- Time to verify
- Time to resolve
- Incident Information (see Figure 13)

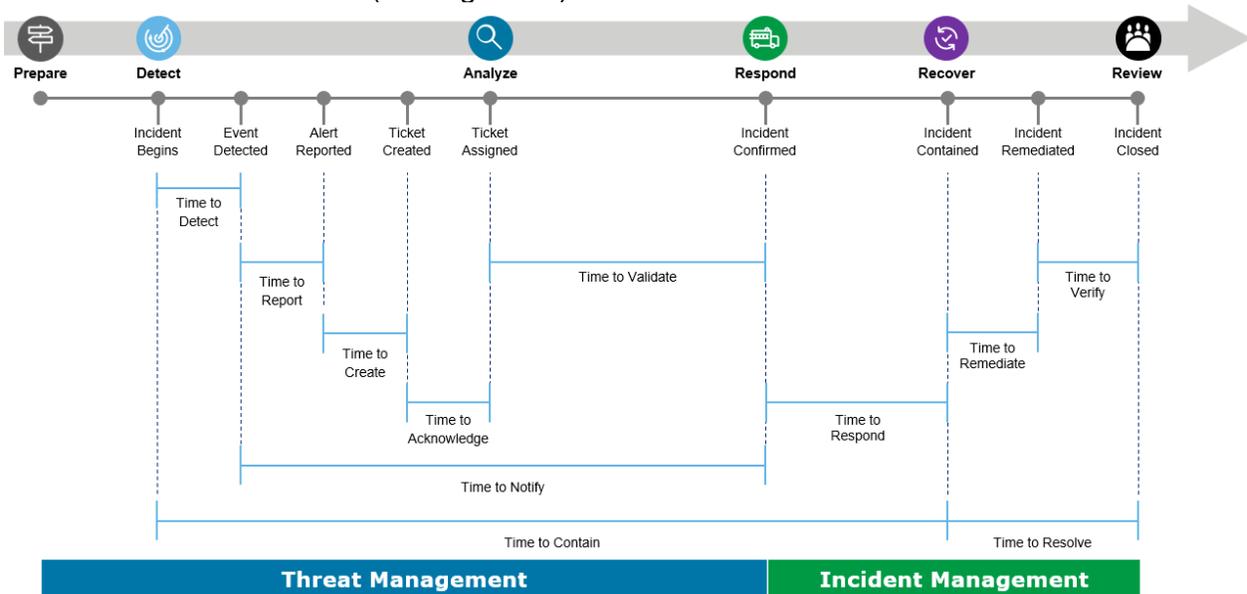


Figure 13: IR Framework



Cybersecurity Incident Response Plan

In the event of a Major Incident, HUD CIRT shall report all details to the SOC Director. The SOC Director is responsible for briefing the Deputy CISO, CISO, and CIO **within one hour**, before reporting the incident to CISA and/or US Congress. If the SOC Director is unreachable, HUD CIRT shall reach out to the same members within one hour as well. IR times per Figure 13 will be documented by the SOC and reported to the Deputy CISO, CISO, and CIO weekly.

5.1 CISA

FISMA 2014 requires HUD to report actual or potential cyber security incidents to the NCCIC/CISA with the required data elements **within one hour** of being identified by HUD. HUD CIRT will report all available incident information at the time of notification and will provided updates as additional information is obtained (see Figure 14)

These information elements are required when notifying CISA of an incident:

1. Identify the current level of impact on agency functions or services (Functional Impact)
2. Identify the type of information lost, compromised, or corrupted (Information Impact)
3. Estimate the scope of time and resources needed to recover from the incident (Recoverability)
4. Identify when the activity was first detected
5. Identify the number of systems, records, and users impacted
6. Identify the network location of the observed activity
7. Identify point of contact information for additional follow-up

Important: Do not include sensitive PII to incident submissions. Any contact information collected will be handled according to the DHS website privacy policy.

8. Submit the notification to CISA

Required for CISA Submission <i>within 1 hour of incident identification</i>	Provide if known at time of submission <i>or as become available</i>
<input type="checkbox"/> Functional Impact	<input type="checkbox"/> Attack Vector(s)
<input type="checkbox"/> Information Impact	<input type="checkbox"/> Indicators of Compromise
<input type="checkbox"/> Recoverability	<input type="checkbox"/> Mitigation Activities Undertaken
<input type="checkbox"/> Time of First Detection	
<input type="checkbox"/> Number of systems, records, and users impacted	
<input type="checkbox"/> Network location of observed activity	
<input type="checkbox"/> Point of Contact information for follow-up	

Figure 14: CISA Notification Requirements

The following information shall also be included if known at the time of submission:

9. Identify the attack vector(s) that led to the incident
10. Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident
11. Provide any mitigation activities undertaken in response to the incident

Within one hour of receiving the report, the NCCIC/CISA will provide the agency with:



Cybersecurity Incident Response Plan

- A tracking number for the incident
- A risk rating based on the NCCIC Cyber Incident Scoring System (NCISS)

Reports may be submitted using the CISA Incident Reporting Form; send emails to soc@us-cert.gov or submit reports via Structured Threat Information eXpression (STIX) to autosubmit@us-cert.gov. Reports can also be submitted through <https://www.us-cert.gov/report>.

The SOC must also be prepared to support the HUD CIO and CISO in providing incident data upon request to satisfy any internal HUD or external Federal agency reporting requirements as needed.

5.2 Congress

FISMA requires HUD to report any Major Incident to Congress **within seven calendar days** of identification. HUD CIRT initially determines if an incident should be designated as major and may consult with CISA to make this determination. Once escalated to CISA, HUD CIRT's determination will be taken into consideration, but CISA is ultimately responsible for declaring an incident as Major.

In addition, HUD must supplement their seven-day report to Congress with another report **no later than 30 calendar days** after if HUD discovers the major incident constitutes a breach. The supplemental report must include:

1. A summary of information available about the breach, including how the breach occurred, and information available to HUD on the date that HUD submits the report
2. An estimate of the number of individuals affected by the breach, including an assessment of the risk of harm to affected individuals affected by the breach, including a risk assessment to the affected individuals based on the report
3. A description of any circumstances that can delay in notifying the affected individuals
4. An estimate of when HUD will be able to provide the notice to affected individuals

6. Plan Testing and Maintenance

This IR Plan is reviewed annually by the SOC Director with support from the SOC major functions. The SOC Director notifies the CIO, CISO, and HUD IT teams of updates. Changes made are documented in the history section. Cybersecurity Leadership consults with technical and business subject-matter experts to identify required changes to the plan.

The IM team tests the IR Plan twice a year. Test plans must include test cases to measure the timeliness and effectiveness of:

- Response for each threat level, including escalations from one level to the next
- Resource engagements, both personnel and logistical (such as teleconference bridge lines)
- Each process activity. It is important to note that not all phases will be required to be performed in all cases. Each potential incident that is identified must be independently assessed and addressed with an appropriate response in line with its type, scope, and severity



Cybersecurity Incident Response Plan

- Implemented according IR processes or Cybersecurity Leadership led IR efforts



Appendix A. Security Operations Roles and Responsibilities

Operational Roles	Responsibilities
Secretary of HUD	<ul style="list-style-type: none"> Provides notice, or designates in writing a senior-level individual to individuals affected by a breach of HUD information resources with the concurrence of the HUD CIO, the SAOP, and the Office of Communications Ensures that the HUD provides timely notice to individuals affected by a HUD breach in accordance with Federal and HUD requirements Ensures that the Office of Congressional Relations notifies Congress about each major incident within 7 days of declaration that it qualifies as a major incident Ensures that the HUD CIO and HUD CISO submit the required annual reporting of information security and cybersecurity incident and cyber-related breach information on time
CPO	<ul style="list-style-type: none"> Directs the identification of PII and the level of impact or sensitivity of compromised PII Informs the SAOP of moderate and high breaches Approves the closure of all other breaches by email
CIO and Principal Deputy CIO	<ul style="list-style-type: none"> Ensures that Departmental policy, program, plans, procedures, and delegations of authority for IM are developed, implemented, disseminated, maintained, and that they comply with FISMA and other applicable Federal requirements Ensures that the Department's annual information security reporting, including information on cybersecurity incidents and cyber-related breaches, is prepared and submitted on time Contacts the SAOP if a major incident is a breach Conducts continual metric assessments of the IM program by analyzing accurate qualitative and quantitative performance data Ensures that the Secretary is informed immediately when a major incident is declared Collaborates with the HUD CISO and the Assistant Secretary for Congressional Relations to provide the appropriate committees of Congress with information about major incidents mandated by FISMA or other Federal requirements in the required timeframes Determines if cybersecurity incident information may be released publicly based on factors such as whether the release of information might negatively affect activities such as criminal investigations
CISO	<ul style="list-style-type: none"> Informs the HUD CIO of major cybersecurity incidents Collaborates with the HUD CIO and the Assistant Secretary for Congressional Relations to provide the appropriate committees of Congress with information about major incidents mandated by FISMA or other Federal requirements in the required timeframes Oversees and ensures compliance with Federal and Departmental policies and requirements for IM and provides guidance and direction to program offices and divisions for adherence Ensures that the Department's IM program and its associated resources and capabilities are developed, implemented, and maintained Ensures that processes are in place to verify that HUD IM, program offices, and divisions create cybersecurity incident POA&Ms and manage them to closure Prepares HUD's annual FISMA report to include cybersecurity incident information, and quarterly reports to meet OMB requirements



Cybersecurity Incident Response Plan

	<ul style="list-style-type: none"> • Notifies and consults with the Inspector General, the SAOP, the Senior Agency Official for Controlled Unclassified Information (CUI), the Chief Financial Officer, the CPO, the OGC, the Assistant Secretary for Congressional Relations, and the Director of OC, as appropriate, regarding cybersecurity incidents • Serves as the Department's principal liaison with CISA and any outside organizations regarding major cybersecurity incidents • Supports the SOC Director in ensuring that the SOC is staffed, trained, and equipped to manage incidents • Ensures that required and relevant IM metrics are regularly collected, analyzed, reported, and used to improve all aspects of the Department's IM program • Ensures that information security awareness training for program offices and divisions users includes user responsibilities for detecting and reporting cybersecurity incidents, including incidents involving PII and CUI
OGC	<ul style="list-style-type: none"> • Develops security policies, 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 • Provides legal counsel, advice, and services in relation to cybersecurity incident investigations • Works with the CISO and OIG to coordinate law enforcement involvement in cybersecurity incidents that involve criminal activity
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 policies are implemented • Develops and maintains HUD's information security program, serving as the department-wide principal advisor on information system security matters • Reviews and approves the processes, techniques, and methodologies planned for securing information system assets
Office of Privacy	<ul style="list-style-type: none"> • Manages the investigation, notification, and mitigation for privacy incidents working with the CISO, OITS, and IOO • Makes joint decisions with the HBNRT regarding the propriety of external notification to affected third parties and the issuance of a press release in High-Impact privacy incidents that occurred and provide recommendations to the SAOP • Makes privacy incident-closure recommendations in consultation with the HBNRT • Prepares 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
IOO	<ul style="list-style-type: none"> • Manages and directs HUD'S IT infrastructure that provides shared services across HUD • Ensures implementation of security components to secure information system assets • Works with the OGC, OIG, and CISO to coordinate law enforcement involvement in incidents that involve criminal activity • Works with CIRT to resolve computer security incidents, including taking certain actions within the infrastructure
OIG	<ul style="list-style-type: none"> • Performs independent evaluations, investigations, and audits of internal and external federal security guidelines/regulations



Cybersecurity Incident Response Plan

	<ul style="list-style-type: none"> • Directs computer forensic investigations upon request in the event criminal intent is suspected • Works with the CISO and OGC to coordinate law enforcement involvement in incidents that involve criminal activity depending on the nature of the violation
SAOP	<ul style="list-style-type: none"> • Holds overall responsibility for the Department's Privacy Program • Serves as chairperson of the HBNRT • Serves as an advocate for privacy IR activities in consultation with the CIO, CISO and Privacy Officer • Advises 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
Operational Roles	Responsibilities
SOC Director	<ul style="list-style-type: none"> • Oversees IM/CIRT actions, performance, and incident escalation • Ensures CIRT has the resources to accurately investigate incidents • Ensures CIRT utilizes a consistent incident handling methodology • Ensures all SOC functional areas collaborate with the IM team to detect, respond, and recover from incidents efficiently • Ensures system owners (including vendors) are able to collect logs necessary for an investigation in support of CIRT • Verifies that HUD's IT vendors adhere to contractual agreements with reporting and response requirements related to cybersecurity incidents • Establishes Service Level Agreements for recovery actions delegated to supporting IT functions and requires follow-up confirmation of their completion in order to ensure timely resumption of normal business activity following an incident • Responds to requests for information (RFIs) from executives and other stakeholders • Establishes a process to prioritize security alerts and reports based upon perceived risk and assigns investigation to IM personnel in accordance with the timelines established in this policy • Reviews and disseminates IR Plan with cybersecurity leadership annually • Ensures that SOC personnel are properly trained to use HUD SOC tools to detect, investigate, respond, and recover from incidents • Reviews and disseminates IM metrics listed in the Metrics Catalog to drive continuous improvement efforts • Can serve as the Incident Commander for major severity events • Accountable for cybersecurity reporting to FISMA and CISA • Ensures the SOC is staffed, trained, and equipped to manage cybersecurity incidents
Incident Commander	<ul style="list-style-type: none"> • Serves as point of contact for major cybersecurity incidents • Responsible for managing and ensuring successful completion of all cybersecurity incidents • Coordinates across HUD cybersecurity and IT teams to ensure rapid response for all "major incidents" • Works with HUD IT and security stakeholders to address threats and restore services to normal operations • Works with SOC Director in fulfilling RFIs from executives and other teams regarding cybersecurity incidents
IM Lead	<ul style="list-style-type: none"> • Responsible for managing and ensuring successful completion of day-to-day IM activities • Leads the IR team



Cybersecurity Incident Response Plan

	<ul style="list-style-type: none"> • Ensures the appropriate staffing coverage is maintained and shift specialists are properly trained • Responsible for cybersecurity reporting requirements to FISMA and CISA • Accountable for the timely dissemination of security information to appropriate stakeholders • Provides cybersecurity incident trend analysis and reporting as required • Communicates regularly with vulnerability management and ASR personnel to maintain awareness of the computing and network environment's current defense posture • Participates in periodic review of security and IT policies, standards, and procedures to ensure leading practices are adopted and implemented in enterprise defenses
IM Team	<ul style="list-style-type: none"> • Responsible for the timely dissemination of security information to appropriate stakeholders • Provide cybersecurity incident trend analysis and reporting as required • Ensure retention of all investigation and incident information in a central repository for at least one year, including all required data points per the established taxonomy in addition to other characteristics • Coordinate IR activities with CIRT • Responsible for cybersecurity reporting requirements to FISMA and CISA
TM Team	<ul style="list-style-type: none"> • Analyze network, application, and user behavior for anomalous events or activity indicative of potential threats • Monitor, correlate, and analyze security log data, recommend remediation actions, and closely collaborate with IM to execute against recommendations • Support IR personnel with any further investigation of incidents for follow-on response and recovery actions
Threat Intel Team	<ul style="list-style-type: none"> • Escalate possible incidents based upon cyber TI reports • Collaborate with HUD CIRT/IM during lessons learned to guide future TI and reconnaissance research.
ASR Team	<ul style="list-style-type: none"> • Support IR personnel in developing recommendations to mitigate or remediate incidents • Prioritize the remediation of identified vulnerabilities to reduce HUD's attack surface • Support risk mitigation by synchronizing, prioritizing, and tracking vulnerability remediation efforts between the SOC, HUD's Vulnerability Management team
IR or CIRT	<ul style="list-style-type: none"> • Manage and respond to cybersecurity incidents that involve HUD systems and data • Perform in-depth analysis of network traffic, system logs, and malware artifacts to determine the appropriate categorization and mitigation techniques required for each case • Review logs periodically to verify if log retention follows HUD log management and/or data retention policies • Help improve the overall security posture of HUD by independently verifying the security of HUD's systems • Responsible for the timely dissemination of security information to the appropriate stakeholders • Coordinate incident validation and investigations with TM personnel • Retrieve forensically sound images of any systems suspected of having been accessed by an unauthorized party for further analysis, either by HUD or another investigative body



Cybersecurity Incident Response Plan

	<ul style="list-style-type: none"> • Participate in periodic reviews of security and IT policies, standards, and procedures to ensure leading security practices are adopted and implemented in enterprise defenses • Gather evidence for the conviction of perpetrators, or disciplining employees • Communicate regularly with vulnerability management and ASR personnel to maintain awareness of the computing and network environment's current defense posture • Interview individuals involved in incident • Act to protect the environment from further impact • Restore the system to its normal business status • Verify the success of restoration operations • Provide public communications guidance on incident impact • Maintain on-call availability
HBNRT	<ul style="list-style-type: none"> • Serve as the privacy incident related breach notification team
Supervisors	<ul style="list-style-type: none"> • Authorize issuance of information system access for their staff • 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"> • Implement and maintain technical controls that enforce operational and managerial controls through mechanisms contained in the hardware, software, or firmware components of the information system • Maintain environment to create a strong technical foundation for enforcement of information system security
ISSO	<ul style="list-style-type: none"> • Ensure that managerial, operational, and technical controls for information system(s) security belonging to the program office are in place and effective • Serve as the principal points of contact 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 • Support all incident handling activities
Service Providers	<ul style="list-style-type: none"> • Ensure and maintain security controls that are compliant with HUD's IT Security Policy and playbooks, including reporting security incidents to the SOC • Support all IR activities
Help Desk	<ul style="list-style-type: none"> • Receive reports of cybersecurity events/incidents • Report all cybersecurity events/incidents to IM/CIRT • Provide users with reporting cybersecurity events/incident guidance
Users	<ul style="list-style-type: none"> • Comply with IT 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 IT Security Awareness Training • Attend the required role-based security training pertaining to those having a security-related role • Report cybersecurity incidents to IM/CIRT according to the established and documented playbooks • Cooperate with the CIRT members in the investigation of cybersecurity incidents • Understand and comply with HUD policies, standards, and playbooks regarding the protection of sensitive HUD information assets • Support all incident handling response activities



Cybersecurity Incident Response Plan

Appendix B. Contact List

Name	Position	Org	Email	Office	Mobile
CNOSC 24hr call center	CNOSC 24hr call center	AT&T	dl-cnoscscoc@att.com	866-829-3974	N/A
HUD CIRT	CIRT	HUD OCIO	CIRT@HUD.gov	-	202-412-7351
Joe Green	HUD POC for CNOSC SOC Manager	AT&T	Joseph.S.Green@hud.gov	-	202-227-9658
Joseph Jones	HUD SOC PM	AT&T	Joseph.L.Jones@hud.gov	-	-
Chris Pruitt	IT Security	HUD OCIO	Christopher.L.Pruitt@HUD.gov	202-402-8322	-
Marcus Harley	IT Security	HUD OCIO	Marcus.A.Harley@hud.gov	202-402-2592	-
Harold Williams	OPSEC	HUD OCIO	Harold.E.Williams@hud.gov	202-402-0087	-
TBD	SOC Director	HUD OCIO	TBD	TBD	TBD
TBD	IM Lead	HUD OCIO	TBD	TBD	TBD
TBD	TM Lead	HUD OCIO	TBD	TBD	TBD
TBD	TI Lead	HUD OCIO	TBD	TBD	TBD
TBD	ASR Lead	HUD OCIO	TBD	TBD	TBD
Haj Ramos	CISO, OIG	HUD OIG	HRamos@hudoig.gov	202.402.2032	202-503-6113
Ladonne White	Chief Privacy Officer	HUD OCHCO	Ladonne.L.White@hud.gov	202-402-3559	
John Crump	CISO, GNMA	HUD GNMA	John.E.Crump@hud.gov	202-426-3250	
Neeraj Saraf	Dir., Data Center Services	HUD OCIO	Neeraj.Saraf@hud.gov	202-402-2674	202-578-5289
Cedric Harris	Dir., Unified Communications	HUD OCIO	Cedric.M.Harris@hud.gov	202-402-6383	TBD
Lisa Clark	Acting DCISO	HUD OCIO	Lisa.A.Clark@hud.gov	202-402-3616	TBD
Juan Sargeant	DCIO, IOO	HUD OCIO	Juan.C.Sargeant@hud.gov	202-402-7431	
Hun Kim	CISO	HUD OCIO	Hun.S.Kim@hud.gov	202-402-7365	TBD
Kevin Cook	DCIO, OCIO	HUD OCIO	Kevin.R.Cooke@hud.gov	202-708-0306	TBD
David Chow	CIO	HUD OCIO	David.C.Chow@hud.gov	202-708-0306	TBD



Cybersecurity Incident Response Plan

Appendix C. Incident Response Framework Data Elements

Figure C1 below depicts the visual phased approach of how incident data elements should be documented throughout the IM lifecycle, as Table C1 defines these data elements as part of the IR lifecycle for Threat and IR analysts to capture. Data elements listed in Table C1 also support IR metrics for reporting and continuous improvement.

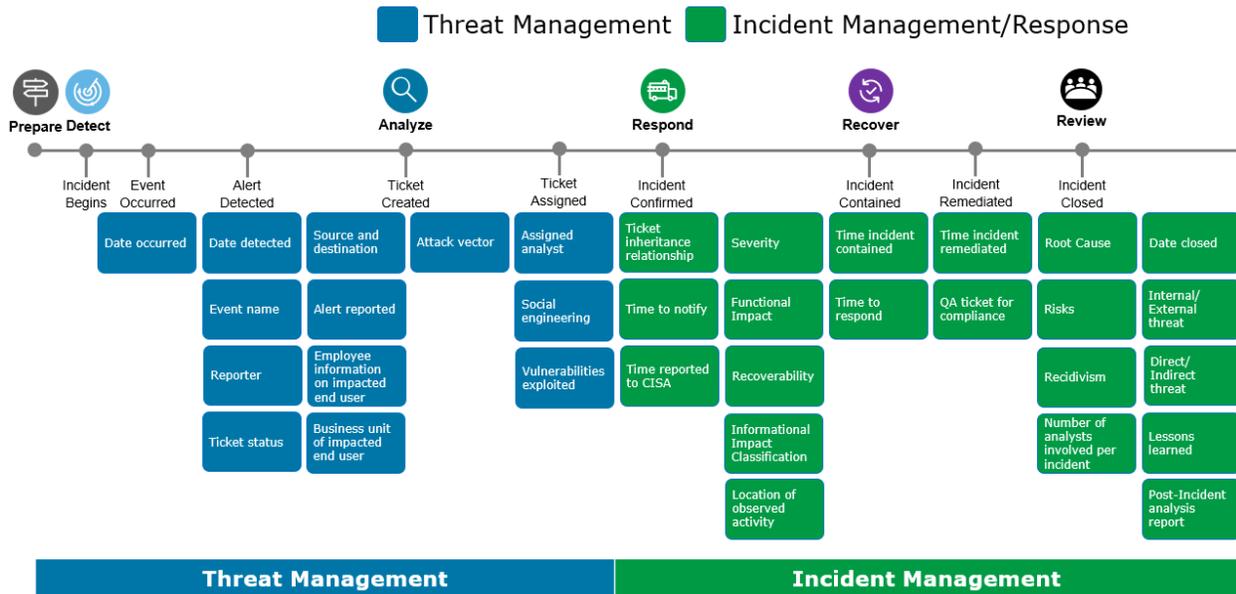


Figure C1: Phased Ticketing

INCIDENT RESPONSE PHASED FRAMEWORK		
Data Element	Phase	Description
Date occurred	Detect	The date/time when the actual event occurred (recorded timestamp)
Date detected	Detect	The date/time when an event was acknowledged by an analyst
Event name detected by monitoring tools	Detect	Name of event or alert rule triggered as defined by cyber tools such as SIEM, IDS/IPS, DLP, threat hunting, and IOC's
Reporter	Detect	The analyst who created the ticket
Ticket Status	Detect	Open, closed, cancelled
Source and destination information	Detect	Resolving source and destination IP's, MAC address, machine names, application
Alert reported	Detect	The date/time the ticket was created in ticketing system



Cybersecurity Incident Response Plan

Employee information of impacted end user	Detect	Business organization, specific team, manager information, assigned office location, role within HUD
Business unit of impacted end user	Detect	Business unit of the impacted user
Attack vector	Analyze	Avenues which a threat actor jeopardizes the integrity, confidentiality, or availability of information or an information system (unknown, attrition, web, email/phishing, external/removable media, impersonation/spoofing, improper usage, loss or theft of equipment, other)
Assigned analyst	Analyze	The analyst that will be working the ticket in the IM phase
Social engineering	Analyze	Yes or no field to indicate if cyber event or alert employed a social engineering technique
Vulnerabilities exploited	Analyze	List of vulnerabilities exploited as defined in the NIST Vulnerability Database. Vulnerabilities exploited may not always be known in the analyze phase but should be validated during the response phase
Ticket inheritance relationship	Respond	Mapping other tickets (parent and child tickets) can be used for multiple events, potential campaigns and data driven initiatives
Time to notify	Respond	Time to notify IR stakeholders such as CISO, CIO, Office of Privacy, and other partner HUD organizations (there can be multiple time to notify fields)
Time reported to CISA	Respond	Note date/time that the incident was reported to CISA (if a major incident)
Severity	Respond	No impact suspected but not identified, privacy data breach, proprietary information breach, destruction of non-critical systems, critical systems data breach, core credential compromise, destruction of critical system. This field is a numerical score based on functional impact, recoverability, information impact, and locations of observed activity. This field is also initially assessed in the Analyze Phase but validated in Response
Functional impact classification	Respond	Identify the current level of impact on agency functions or services. This field is also initially assessed in the Analyze Phase but validated in Response
Recoverability	Respond	Estimate the scope of time and resources needed to recover from the incident. This field is also initially assessed in the Analyze Phase but validated in Response
Information impact classification	Respond	Identify the type of information lost, compromised, or corrupted. This field is also initially assessed in the Analyze Phase but validated in Response
Location of observed activity	Respond	The logical location of observed malicious activity within the network environment



Cybersecurity Incident Response Plan

Time incident contained	Recover	Duration of how long it took for the incident to contained/not propagate within the network
Time to respond	Recover	Duration of how long it took for analyst to respond between event detected and the response phase. This also includes notification to affected HUD stakeholders (i.e. system owners, business units, OITS leadership)
Time incident remediated	Recover	Duration of long it took for incident to be completely remediated
QA ticket for compliance	Recover	Quality assurance performed on ticket to ensure data integrity and government compliance
Root cause	Review	Reviewing the incident and determining what was the root cause of the incident in the first place
Risks	Review	Risk that were associated with the incident as well as risks with remediation (e.g. impact to business operations, customers, etc.)
Recidivism rate	Review	Repeated incident
Date closed	Review	Date/time incident ticket closed (e.g. resolution from CISA, HUD leadership)
Internal/External threat	Review	Insider threat or external actor
Direct/Indirect threat	Review	Incident is direct threat targeting HUD (e.g. spear phishing) or indirectly targets HUD (e.g. commodity malware drive-by)
Number of analysts involved per incident	Review	The number of analysts involved in the incident once the incident is remediated
Post-Incident Analysis Report	Review	Post-Incident Analysis Report provides information to HUD and appropriate external partners with a summary of an incident, impact to the organization, as well as lessons learned and areas of improvement. In the incident ticket, this would be a “complete” or “not completed” field
Lessons learned	Review	Major takeaways; issues identified as well as areas to sustain and/or improve with respect to cybersecurity and IR capabilities. Also include follow-up actions that can improve the organizations security posture. In the incident ticket, this would be a “complete” or “not completed” field

Table C1: Incident Data Elements to Document



Appendix D. Log Artifact Checklist

Important: If any devices are added to the HUD environment, add the device to the list below

	Artifact Type	Logs Collected?
1	Security Device Logs	
1.1	IDS/IPS	<input type="checkbox"/>
1.2	Firewall/Gateway	<input type="checkbox"/>
1.3	Data Loss Prevention Logs	<input type="checkbox"/>
1.4	Endpoint Anti-Virus	<input type="checkbox"/>
1.5	Other Endpoint Security	<input type="checkbox"/>
1.6	Other Security Devices	<input type="checkbox"/>
2	Access Logs	
2.1	On-Premise Active Directory	<input type="checkbox"/>
2.2	Azure Active Directory	<input type="checkbox"/>
2.3	Azure Sign-in Logs	<input type="checkbox"/>
2.4	System-specific authenticate/authorize	<input type="checkbox"/>
2.5	Host-specific authenticate/authorize	<input type="checkbox"/>
2.6	Salesforce Logs	
2.7	Other relevant access logs	<input type="checkbox"/>
3	HUD Cloud Environments	
3.1	Web App Firewall on Azure Application Gateway	<input type="checkbox"/>
3.2	Network Security Groups flow logs (ingress and egress IP traffic through an NSG)	<input type="checkbox"/>
3.3	Control/management logs (Create/Update/Delete Operations)	<input type="checkbox"/>
3.4	Data plane logs (Virtual Machines within EDM)	<input type="checkbox"/>
3.4.1	Windows OS local Logging	<input type="checkbox"/>
3.4.2	Linux OS local logging	<input type="checkbox"/>
3.4.3	SQL Server Logs SQL Trace logs (schema change history) SQL Maintenance Plan (backup history)	<input type="checkbox"/>
3.5	Processed Events	<input type="checkbox"/>



Cybersecurity Incident Response Plan

	Azure Security Center alerts	
3.6	AWS CloudWatch Logs	
4	Typical Components in EDM	
4.1	Databricks workspace audit logs	<input type="checkbox"/>
4.2	Talend job logs	<input type="checkbox"/>
4.3	Other	<input type="checkbox"/>
5	Office 365 Security & Compliance Center	
5.1	SharePoint	<input type="checkbox"/>
5.2	OneDrive	<input type="checkbox"/>
5.3	Exchange	<input type="checkbox"/>
5.4	Power BI	<input type="checkbox"/>
5.5	Teams	<input type="checkbox"/>
5.6	Yammer	<input type="checkbox"/>
6	Access Control Lists (who/what and permissions)	<input type="checkbox"/>
7	Device snapshots or backups	<input type="checkbox"/>
8	Reports, statements, interviews, emails	
8.1	Incident alerts from MSSP	<input type="checkbox"/>
8.2	Initial incident description/write up	<input type="checkbox"/>
9	List of Relevant Users	<input type="checkbox"/>



Cybersecurity Incident Response Plan

Appendix E. SOC Tools & Technologies Listing

The following list are the main tools and technologies used by the SOC

Tool/Technology	Purpose	Owner
Archer	An integrated platform for managing multiple dimensions of risk, including IT, operational, third-party, resiliency, and compliance risk. Provides vulnerability scan data and their severity levels for SOC review and analysis	IOO
Blue Coat Proxy	A solution that provides protection against web and network-based threats, enables cloud data protection, provides load balancing, and allows business policy control across enterprise and cloud, (including web, social and mobile networks)	IOO/Operational Security
CA Service Desk	Ticketing system to track incidents. System of record for incident data	OITS
Cisco IPS	An inline, deep-packet inspection feature that effectively mitigates a wide range of network attacks	IOO/Operational Security
Einstein 3 Accelerated (E3A)	Developed by the United States Computer Emergency Readiness Team as an intrusion detection system that monitors network gateways for government agencies and departments	HUD & DHS
McAfee DLP	Safeguards intellectual property and ensures compliance by protecting sensitive data on endpoint systems. Provides alerts when data loss rules are triggered	HUD IOO/Unified Communications
McAfee Endpoint Security	Solution that integrates endpoint threat protection, detection, investigation, and response. Protects and alerts against malware, ransomware and ensures safe browsing with web protection and filtering for endpoints	HUD IOO/Unified Communications
McAfee ePO	Software that centralizes and streamlines management of endpoint, network, data security, and compliance solutions	HUD IOO/Unified Communications
Microsoft O365 DLP	Identifies, monitors, and automatically protects sensitive information across Office 365	HUD IOO/Unified Communications
Nessus	Vulnerability scanner that identifies the vulnerabilities that need attention for remediation	OITS
Splunk	Software platform that searches, analyzes and visualizes machine-generated data gathered from almost every endpoint	OITS
Threat Insights	Aggregates data across multiple TI sources and uses this data to detect malicious activity and threat actors.	OITS

The following are Open Source tools available for SOC personnel to use to analyze incidents
Disclaimer: Only use if artifacts DO NOT contain sensitive information e.g. PII

Tool/Technology	Purpose
CentralOps	Domain dossier with Whois lookup
Cisco Talos	An open source and research tool that provides IP information and Domain reputation



Cybersecurity Incident Response Plan

Cuckoo	A sandbox with dynamic automated malware analysis
Hybrid Analysis	A free automated malware analysis tool
Malware Traffic Analysis.net	An open source security research site that provides PCAP and malware samples
NFDUMP	A set of tools that collects, process, and analyzes NetFlow data
OSSEC	Open source Host Intrusion Detection System with various operating systems
Robtex	An open source research tools that gathers public information about IP numbers, domain names, host names, Autonomous systems, routes etc.
SANS SIFT	An Ubuntu based computer forensics distribution that can perform digital forensics and IR analysis
Security Onion	Linux distribution for threat hunting, enterprise security monitoring, and log management (used in CS3 stack)
VirusTotal	An open source service that analyzes files and URLs enabling the detection of malicious content
WireShark	A network protocol analyzer used for analysis, troubleshooting, and software and communications protocol development (used in CS3 stack)
Zeek (BRO IDs)	A free and open-source software network analysis framework (used in CS3 stack)



Appendix F. Post-Incident Analysis Report Template

The Post-Incident Analysis Report provides information to HUD and appropriate external partners with a summary of an incident, impact to the organization, as well as lessons learned and areas of improvement. All Major Incidents will require a Post-Incident Analysis report to be completed. Post-Incident analysis for non-major incidents should be completed at the SOC Director’s discretion.

Post-Incident Report			
Incident Information		Date/Time (ETC)	
Ticket Number	<i>Unique identifier</i>	Occurred	
Event Detected	<i>Rule triggered or SIEM event entry</i>	Detected	
Affected Business Unit		Ticket created	
Affected app/system		Ticket closed	
Notes <i>Commentary on the timeline of events to include notification of internal HUD stakeholders and external partners</i>			
Impact & Severity Assessment			
Functional Severity Level	<i>Reference Table 2</i>	Functional Severity Score	<i>Reference Table 2</i>
Information Severity Level	<i>Reference Table 3</i>	Information Severity Score	<i>Reference Table 3</i>
Recoverability Severity Level	<i>Reference Table 4</i>	Recoverability Severity Score	<i>Reference Table 4</i>
Location of Observed Activity	<i>Reference Table 5</i>	Locations of Observed Activity Score	<i>Reference Table 5</i>
Total Severity Level	<i>Reference Table 1</i>	Total Severity Score	<i>Reference Table 1</i>
Major Incident? <i>(check if yes)</i>	<input type="checkbox"/>		
Cause Analysis and Threat Information			
Attack Vector	<i>Reference Table 6</i>		
Root Cause	<i>Underlying cause or causes to an incident such as unpatched vulnerability, lack of system or access controls</i>		
Threat Characterization	<i>(internal/external, direct/indirect)</i>		
Other tickets/events	<i>(list of associated tickets)</i>		
Recidivism	<i>Has the incident occurred before?</i>		



Cybersecurity Incident Response Plan

Notes <i>Commentary on the source and destination of the incident or threat as well as how vulnerabilities or lack of security controls were exploited. Also note if the incident or threat spread to other areas of the HUD network and how?</i>	
Remediation & Recovery	
How was the incident contained?	<i>List activities and partnerships used to sweep and contain the incident.</i>
How was the incident eradicated?	<i>List activities, partnerships, and technologies used to remediate the incident and ensure no other HUD systems assets could be affected.</i>
Recovery	<i>Has HUD recovered from the incident or is recovery on-going? How long did recovery take? What resources were used to recover? Did recovery require additional assistance (e.g. re-purpose of other personnel, contract support)</i>
General Comments, Notes	
<i>List any additional notes such as areas of improvement and practices that must be sustained to properly respond and recover from future incident.</i>	



Appendix G. Lessons Learned Template

The Lessons Learned report will be a sub-set of the Post-Incident Analysis report. The Lessons Learned report will contain recommendations for future areas of improvement, practices that HUD must sustain in the future, and recommendations on implementing controls, processes, or technology to defend against future similar incidents.

Lessons Learned	
<p>Prompts:</p> <ul style="list-style-type: none"> • How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate? • What information was needed sooner? • Were any steps or actions taken that might have inhibited the recovery? • What would the staff and management do differently the next time a similar incident occurs? • How could information sharing with other organizations have been improved? • What corrective actions can prevent similar incidents in the future? • What precursors or indicators should be watched for in the future to detect similar incidents? • What additional tools or resources are needed to detect, analyze, and mitigate future incidents? 	
Areas to Improve	
Business unit, system owner, vendor, user(s), etc.	
SOC	
Areas to Sustain	
Business unit, system owner, vendor, user(s), etc.	
SOC	



Cybersecurity Incident Response Plan

Appendix H. Authorities and References

1. DHS, CISA Federal Incident Notification Guidelines, April 1, 2017
2. Federal Information Security Modernization Act of 2014 (FISMA), 44 United States Code (U.S.C.) §3551, et seq., December 18, 2014
3. Handbook for Safeguarding Sensitive PII. Privacy Policy Directive 047-01-007, Revision 3. DHS Privacy Office. December 4, 2017
4. HUD IT Security Policy, HUD Handbook 2400.25 Rev 5
5. HUD Breach Notification Response Plan
6. NIST, FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006 NIST, Interagency Report (IR) 7298 Revision 2, Glossary of Key Information Security Terms, May 2013
7. NIST, SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 with updates as of January 22, 2015
8. NIST, SP 800-61 Revision 2, Computer Security Incident Handling Guide, August 2012
9. OMB, Circular A-130, Managing Information as a Strategic Resource, July 28, 2016
10. OMB, Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government, October 30, 2015
11. OMB, Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017
12. OMB, Memorandum M-19-02, Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements, October 25, 2018
13. Presidential Policy Directive 41 (PPD-41) - United States Cyber Incident Coordination



Cybersecurity Incident Response Plan

Appendix I. Glossary / Definitions

- a) Alert – An indicator of malicious activity based upon the aggregation, correlation, and/or analysis of events.
- b) Breach – The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for another than authorized purpose. (Source: OMB M-17-12)
- c) Compromise – Disclosure of information to unauthorized persons, or a violation of the security Policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. (Source: NIST IR7298 Revision 2)
- d) Cybersecurity Incident – See “Incident.”
- e) 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. (Source: NIST SP 800-61 Revision 2) Note: Events with negative consequences are referred to as adverse events.
- f) Incident – An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security playbooks, or acceptable use policies. (Source: FISMA) Note: An occurrence may be identified as an incident, but later identified as a breach once it is determined that PII is involved. Also, “incident” encompasses more specific terms such as “cybersecurity incident,” “information security incident,” “computer security incident,” spillage of CNSI, or exposure of CUI.
- g) IM – The CIRT administers the IR program to include monitoring, tracking, response coordination and reporting of HUD computer security incidents. HUD-IM 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.
- h) Information Security Incident – See “Incident.”
- i) Major Incident – Is either:
 - (1) Major incident – As defined by OMB M-17-05, a "major incident" is any incident that is likely to result in demonstrable harm to the national security interests, foreign



Cybersecurity Incident Response Plan

relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. Using the DHS NCISS this includes Level 3 events (orange), defined as those that are “likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence”; Level 4 events (red), defined as those that are “likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties”; and Level 5 events (black), defined as those that “pose an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons.”

- (2) A breach that involves PII that, if exfiltrated, modified, deleted, or otherwise compromised is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. (Source: OMB M-19-02)
- j) PII – Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (Source: NIST SP 800-122)
- k) 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.
- l) Sensitive PII – 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.
- m) Significant Cyber Incidents – they are likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties or public health and safety of the American people. These significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors as appropriate.
- n) Threat – The potential source of an adverse event. (Source: NIST SP 800-61 Revision 2)



Cybersecurity Incident Response Plan

- o) Vulnerability – A weakness in a system (e.g., application, system security playbooks, hardware, design, or internal controls) that could be exploited or misused. (Source: NIST SP 800-61 Revision 2)



Cybersecurity Incident Response Plan

Appendix J. Acronyms

Acronym	Definition
ASR	Attack Surface Reduction
CDM	Continuous Diagnostics and Monitoring
CIRT	Cybersecurity Incident Response Team
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CUI	Controlled Unclassified Information
Department	Department of Housing and Urban Development
DMZ	demilitarized zone
DHS	Department of Homeland Security
DLP	Data Loss Prevention
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
HBNRT	HUD Breach Notification Response Team
HUD	Department of Housing and Urban Development
IOCs	Indicators of Compromise
IPs	Internet Protocols
IM	Cybersecurity Incident Management
IOO	Infrastructure and Operations Center
IP	Internet Protocol
IR	Cybersecurity Incident Response
IR Policy	Cybersecurity Incident Response Policy
IR Plan	Cybersecurity Incident Response Plan
ISSOs	Information System Security Officers
IT	Information Technology
MBR	master boot record
NCCIC	National Cybersecurity and Communications Integration Center
NCISS	NCCIC Cyber Incident Scoring System
NIST	National Institute of Standards and Technology
OGC	Office of General Counsel
OIG	Office of Inspector General
OITS	Office of Information Technology Services
OMB	Office of Management and Budget



Cybersecurity Incident Response Plan

Acronym	Definition
TM	Threat Management
PII	Personally Identifiable Information
RFI	Request for Information
SAOP	Senior Agency Official for Privacy
SIEM	Security Incident and Event Management
SPII	Sensitive Personally Identifiable Information
TI	Threat Intelligence
URL	Uniform Resource Locator