FACILITY-RELATED CONTROL SYSTEMS EVENT/INCIDENT RESPONSE PLAN (EIRP)

[Replace ESTCP Logo with Organization Logo]

June 20, 2017

Organization Address

City, State, Zip Code

Controlled Unclassified Information (CUI)

Table of Contents

EXECUTIVE SUMMARY

The [Organization] is a private company with numerous contracts with local, state and federal agencies, providing public policy research, and software development on a broad range of topics. The [Organization] operates internal and external servers and networks, both on behalf of government clients, and for its own use. The range of data stored, analyzed, transported and processed includes Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII). The range of information types handled by [Organization] information systems requires a robust and dynamic Event/Incident Response Plan (EIRP) effort, which itself is part of overall effort to maintain a security information environment that protects the confidentiality, integrity and available of [Organization] systems and data, as well as those belonging to our clients. The [Organization] Corporate Information System Security Plan (ISSP) outlines the policies, procedures, baseline security controls, privacy controls and security assurances employed to provide the necessary protection. This document describes the procedures for handling a variety of security incidents; defines a security incident; categorizes the types of security incidents, and the timeframe for reporting each; defines incident response levels; outlines the responsibilities for various roles; and delineates the specific procedures to be followed for each role in the event of a security incident.

Prepared by

Identification of Organization that this Document Prepared by		
Logo	Organization Name	
	Street Address	
	Suite/Room/Building	
	City, State Zip	

Prepared for

Identification of Organization that this Document was Prepared for		
Logo	Organization Name	
	Street Address	
	Suite/Room/Building	
	City, State Zip	

TEMPLATE REVISION HISTORY

Date	Page(s)	Description	Author
06/20/2017	All	Initial Document - The document was modeled after the FedRAMP template but modified to add the new US-CERT Incident Reporting Form and the USCYBERCOM Incident Reporting process	Michael Chipley

Controlled Unclassified Information (CUI)

ABOUT THIS DOCUMENT

This document has been developed to provide guidance and procedures for [Organization] Event/Incident communications.

HOW THIS DOCUMENT IS ORGANIZED

This document is divided into three sections. Some sections include subsections.

Section 1	Describes the introduction and provides an overview and includes the purpose of the document as well as the authorities and standards.
Section 2	Describes the Event/Incident response plan objectives.
Section 3	Describes the Event/Incident response plan roles and responsibilities, severity levels for both US-CERT and USCYBERCOM

1. INTRODUCTION AND PURPOSE

1.1 DEFINTION

A computer security or privacy event/incident is an occurrence having actual or potentially harmful effects on an information system or an individual and/or their data. Any attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations is an information system is considered an "event/incident". This could also be defined as the loss of data through theft or device misplacement, loss or misplacement of a hardcopy document, misrouting of email, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction. Any occurrence that has the potential for jeopardizing the confidentiality, integrity or availability of an information system or its associated data that is stored, transmitted or processed is a security or privacy incident.

1.2 POTENTIAL EVIDENCE OF A SECURITY INCIDENT

Users of [Organization]'s information systems are responsible for identifying and reporting any suspicious activity that may indicate a possible security incident. Some incidents are subtle, and require analysis and technical review to ascertain not only the type of incident that has occurred, but whether an incident has occurred at all. At other times, certain behaviors by computers, servers and devices connected to an information system can indicate a security incident:

- Password changes you didn't initiate (you can't log in) or requests to share your password,
- E-mail activity to you or that is received in your mailbox,
    - Responses to e-mail that was not sent by you,
    - Large volumes of spam, or
    - Large numbers of messages you didn't send
- Browser home page changes or pop-up ads that can't be closed,
- New desktop icons appearing at login,
- Inability to connect to Internet servers (web- or application-sites),
- Workstation infection from a virus, worm or Trojan, adware, or spyware
- Sudden workstation slowdowns,
- File additions, changes, or deletions,
- Noticeable decreases in hard drive space, or
- Sudden increases in hard drive or network activity.

2. EVENT/INCIDENT REPORTING PROCEDURE

2.1 CATEGORIES OF EVENTS/INCIDENTS

Event/Incidents are placed into categories at [Organization] to identify not only the proper response, but to define a timeframe for reporting that must be adhered to by all information system users. These categories are defined for [Organization], but are similar to categories used by our federal agency clients.

Submitting Incident Notifications

The information elements described in steps 1-7 below are required when notifying US-CERT of an incident:

1. Identify the current level of impact on agency functions or services (Functional Impact).

Functional Impact – A measure of the impact to business functionality or ability to provide services
NO IMPACT – Event has no impact.
NO IMPACT TO SERVICES – Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers.
MINIMAL IMPACT TO NON-CRITICAL SERVICES – Some small level of impact to non- critical systems and services.
MINIMAL IMPACT TO CRITICAL SERVICES –Minimal impact but to a critical system or service, such as email or active directory.
SIGNIFICANT IMPACT TO NON-CRITICAL SERVICES – A non-critical service or system has a significant impact.
DENIAL OF NON-CRITICAL SERVICES – A non-critical system is denied or destroyed.
SIGNIFICANT IMPACT TO CRITICAL SERVICES – A critical system has a significant impact, such as local administrative account compromise.
DENIAL OF CRITICAL SERVICES/LOSS OF CONTROL – A critical system has been rendered unavailable.
NO IMPACT – Event has no impact.

2. Identify the type of information lost, compromised, or corrupted (Information Impact).

Information Impact – Describes the type of information lost, compromised, or corrupted.
NO IMPACT – No known data impact.
SUSPECTED BUT NOT IDENTIFIED – A data loss or impact to availability is suspected, but no direct confirmation exists.
PRIVACY DATA BREACH – The confidentiality of personally identifiable information (PII[6]) or personal health information (PHI) was compromised.
PROPRIETARY INFORMATION BREACH – The confidentiality of unclassified proprietary information[7], such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
DESTRUCTION OF NON-CRITICAL SYSTEMS – Destructive techniques, such as master boot record (MBR) overwrite; have been used against a non-critical system.
CRITICAL SYSTEMS DATA BREACH - Data pertaining to a critical system has been exfiltrated.
CORE CREDENTIAL COMPROMISE – Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated.
DESTRUCTION OF CRITICAL SYSTEM – Destructive techniques, such as MBR overwrite; have been used against a critical system.

3. Estimate the scope of time and resources needed to recover from the incident

(Recoverability).

Recoverability – Identifies the scope of resources needed to recover from the incident
REGULAR – Time to recovery is predictable with existing sources
SUPPLEMENTED – Time to recovery is predictable with additional resources.
EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed.
NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).

4. Identify when the activity was first detected.

5. Identify the number of systems, records, and users impacted.

Potential Impact
Minimal
Low
Moderate
High
Severe

6. Identify the network location of the observed activity.

Location of Observed Activity: Where the observed activity was detected in the network.
LEVEL 1 – BUSINESS DEMILITERIZED ZONE – Activity was observed in the business network's demilitarized zone (DMZ)
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.
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.
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.
LEVEL 5 – CRITICAL SYSTEM MANAGEMENT – Activity was observed in high-level critical systems management such as human-machine interfaces (HMIs) in industrial control systems.
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.
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.
UNKNOWN – Activity was observed, but the network segment could not be identified.

Actor Characterization
Hactivists – those who subversively use computers and computer networks to advance a political agenda.
Unwitting Insider – a person with legitimate access to a computer system or network who unknowingly assists in transmitting information.
Criminal – A criminal attack or breach against an individual or organization.
Unknown – An attack from an unidentified source.
Witting Insider – a person with legitimate access to a computer system or network who makes a conscious decision to transmit information.
APT – a network attack in which an unauthorized person gains access to a network and remains undetected for a long period of time.
APT (Targeted) – a network attack in which an unauthorized person gains access to a network and remains undetected for a long period of time while directly targeting an individual or organization.

Observed Activity
None
Prepare - Prepare actions are actions taken to establish objectives, intent, and strategy; identify potential targets and attack vectors; identify resource requirements; and develop capabilities.
Engage - Engage activities are actions taken against a specific target or target set prior to gaining, but with the intent to gain access to the victim's physical or virtual computer or information systems, networks, and data stores.
Presence - Presence is the set of actions taken by the threat actor once access to the target physical or virtual computer or information system has been achieved. These actions establish and maintain conditions for the threat actor to perform intended actions or operate at will against the host physical or virtual computer or information system, network, or data stores.
Effect - Effects are outcomes of a threat actor's actions on a victim's physical or virtual computer or information systems, networks, and data stores

7. Identify point of contact information for additional follow-up.

8. Submit the notification to US-CERT.

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

9. Identify the attack vector(s) that led to the incident.

Attack Vector
Unknown - Cause of attack is unidentified.
Attrition - An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
Web - An attack executed from a website or web-based application
Email/Phishing - An attack executed via an email message or attachment.
External/Removable Data - An attack executed from removable media or a peripheral device.
Impersonation/Spoofing - An attack involving replacement of legitimate content/services with a malicious substitute.

Improper Usage - Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
Loss or Theft of Equipment - The loss or theft of a computing device or media used by the organization
Other - An attack method does not fit into any other vector

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.

2.2 PRIOR TO REPORTING AN EVENT/INCIDENT

In the crucial moment's right after you discover an event/ incident, there is opportunity to either greatly help, or hurt the IT security professionals who will investigate the event/incident. Here are some guidelines for how to proceed in the moments after you realize a event/incident may have occurred, or is underway:

- If the event/incident involves a password which has been compromised, first CHANGE the password immediately, THEN report the incident, according to the guidelines outlined below in this document.
- DO NOT continue working. Instead, come to a graceful work stoppage and save your work to a designated online or network resource.
- THEN, close all applications, if possible, and shutdown your computer.
- DO NOT resume using your computer until it has been cleared by the IT support personnel, or other members of the Computer Incident Response Team (CIRT).
- And finally, DO NOT discuss the event/incident with anyone except the CIRT, as you may be speaking to someone involved in the event/incident. Also, in a event/ incident, when interviewing individuals, it is better if people recall what happened, as opposed to what they heard someone else describe.

2.3 REPORTING AN INCIDENT

First, notify [Organization] IT Support Team **by phone** using the following dial tree, in this order.

(1) **IT Systems Manager** [Name]: desk:
mobile:

(2) **IT Support Specialist** [Name]: desk:
mobile:

If this incident involves an [Organization] application, or software, or if you were unable to contact IT Support Team members above, next contact:

(3) **Software Dev. Manager** [Name]: desk:
mobile:

If you are unable to contact the above individuals, notify [Organization]'s Executive Management:

(4) **CISO** [Name]: desk:

mobile:

(5) **COO** [Name]: desk:
mobile:

(6) **CEO/President** [Name]: desk:
mobile:

Before submitting any paperwork, creating a Help Desk ticket, or anything else, it is imperative you get IT Support involved immediately, in case the attack is on-going, and will allow them time to witness and gather information while the situation is in progress. AFTER notifying IT Support, create a Help Desk Support ticket, and notify the rest of the individuals listed on the form.

The form used at [Organization] to report a potential security incident is the aptly named, “Security Incident Reporting Form”. This form can be found on the [Organization] corporate SharePoint in the ***“Forms and Templates”*** section of the ***[Organization] Corporate Team Site***. (See Attachment 1).

When reporting any incident, it is imperative that attention to detail is exercised. Accurately note times, dates, names, descriptions of activities and other pertinent details, so that as much precision as possible can be communicated on the form. Pay particular attention to:

- Your identifying information, such as name, location, phone, name of computer, etc.
- A thorough and specific description of the suspect activity.
- How the suspicious activity differs from normal activity.
- Details of the activity, e.g – dates, times, IP address or other identifying IT information, if known,
- Any other pertinent information that can be gathered in the process, without making the situation worse, or notifying the person responsible that the security incident has been noticed.

Upon completion of the form, scan it and send a copy to the following roles:

- **Corporate Information Systems Security Manager (ISSM)**
- **Corporate Information Systems Security Officer (ISSO):**
- **CISO**
- **COO**
- **CEO**

3. Incident Reporting Process

3.1 ROLES AND RESPONSIBILITIES

3.1.1 SYSTEM USER

The System User can be an [Organization] employee, vendor, subcontractor or client who has been authorized access to an [Organization] information system.

3.1.1.1 RESPONSIBILITIES:

(1) Take careful notes of all details related to the security incident.
(2) Report security incident(s) to the appropriate point of contact (POC), i.e, [Organization] CIRT, IT Support Help Desk or [Organization] project manager, in the case of clients.

(3) Assist CIRT by providing accurate and detailed information, and answering any questions posed as honestly and forthrightly as possible.

3.1.2 [ORGANIZATION] IT SUPPORT

The IT Support members are responsible for all IT systems at [Organization]. As such, they are the eyes and ears on the ground, and most likely to be able to spot unusual or suspicious activity. More often than not, they will be the first to recognize a security incident. However, in the case where an incident is first observed by a system user, the IT Support members' most important role is to listen carefully, and not jump to conclusions. Further, as with the system user, and all others, it is imperative to take careful notes, and pay attention to detail.

3.1.2.1 RESPONSIBILITIES:

(1) Be available to receive phone calls at desk or mobile numbers during business hours and within reason during off-hours. The IT Support team can be reached via group email at: [IT support team email].
(2) Generate a Help Desk ticket, if the user has not done so already to document and aggregate information concerning the security incident as soon as possible.
a. Update the Help Desk ticket with new information as it becomes available.
b. Close/Resolve the Help Desk ticket upon resolution of the security incident.
(3) Take careful notes of all details related to the security incident.
(4) Determine if the incident involves PII, PHI or SBU data.
(5) Serve as member of [Organization]'s CIRT.
(6) Keep Executive Management apprised of all aspects of the security incident through to completion.
(7) Update the IT Support Standard Operating Procedures (SOP) with new procedures or information resulting from any security incidents resolved.

3.1.3 [ORGANIZATION] COMPUTER INCIDENT RESPONSE TEAM (CIRT)

In most cases, the CIRT will be comprised of:

- All members of [Organization] IT Support (in-house and contract support)
- [Organization] ISSM
- Security professionals, as designated by vendors or subcontractors for information systems outsourced, or cloud-based, or otherwise external to [Organization]'s core information system located at [Organization] corporate HQ. These individuals must have been duly vetted and authorized to have administrative or privileged access to either [Organization]'s systems, external systems that interconnect with [Organization] systems, or systems managed or hosted on behalf of [Organization] by 3rd parties.

While these basic member groups can, at any time, comprise the CIRT, by nature, this team is flexible, and will be made up of individuals with prior authorized privileged access to [Organization]'s systems, as warranted.

3.1.3.1 RESPONSIBILITIES:

(1) The CIRT will notify Executive Management, if not already notified of the nature and extent of the incident at the earliest feasible time.
(2) Serves as the focal point for all communications related to the security incident

(3) Develop and implement component-level plans and procedures to address security incidents, in accordance with this document, [Organization] SOPs, and applicable laws, directives, standards, procedures and guidelines

3.1.4 INFORMATION SYSTEMS SECURITY MANAGER

The ISSM as head of the IT Support department is the focal point and point of contact for both support-related IT issues, and security/privacy issues.

3.1.4.1 RESPONSIBILITIES:

(1) Serves as Team Lead for the CIRT.
(2) Notifies and assembles the CIRT.
(3) Receives the Security Incident Reporting Form, and ensures it is complete, accurate and contains enough information to do a thorough analysis of the root cause of the incident.
(4) Assigns the associated Help Desk ticket to the proper CIRT team member for resolution.
(5) Apprises Executive Management and the [Organization] Management team of ramifications to other system(s) and priorities, as well as the basic facts of the incident at hand.
(6) Recommends a course of action to remediate the issue, then in capacity as CIRT Team Lead, supervises and coordinates the implementation of the management approved course of action.
(7) Drafts (or assigns the task of drafting) the Security Incident Investigation Form, and ensures it is complete, thorough and accurate.
(8) Presents the Security Incident Investigation Report to Executive Management and the HR Director.
(9) Documents the security incident in the “Security Incident Tracking” database in SharePoint, located in the IT Support SharePoint site.
(10) Ensures all phases of remediation, through to documentation are completed.
(11) Updates the Help Desk ticket as needed, and ensures the Help Desk ticket is resolved.

3.1.5 INFORMATION SYSTEMS SECURITY OFFICER

The ISSO serves as the corporate level IT manager. The IT Systems Manager and Software Development Manager report directly to the IT Director. The ISSO has oversight over all aspects of the IT Department; sets priority for IT projects; and approves all work-plans. At [Organization], the ISSO is a member of Executive Management, and sets the direction for IT efforts as they relate to [Organization]’s business mission of public policy research, and the related software development.

3.1.5.1 RESPONSIBILITIES:

(1) Serves on the CIRT.
(2) Provides guidance and oversight for all security issue resolution, particularly as it affects other departments such as Research, Accounting, HR, etc.
(3) Approves the work plan for remediation of security incidents
(4) Reviews and approves changes to configuration(s), particularly as they impact existing Authority to Operate (ATO).

3.2 US-CERT INCIDENT HANDLING FOR DIFFERENT LEVELS OF SEVERITY

Severity Level	NCCIC Description	[Organization] Description	Handling Procedure
20 Baseline (Negligible)	A Baseline–Negligible priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	User reported event. Incident status not yet confirmed.	Security Incident Reporting Form completed; CIRT assembled to review and analyze if an incident exists, and if so, the scope of security incident. **Notification:** [Organization] Executive Management
35 Baseline (Minor)	A Baseline–Minor priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. The potential for impact, however, exists and warrants additional scrutiny.	Incident effects are localized. No more than one or two computers affected. No major The PMC Group systems affected. Examples include non-mailing viruses, receipt of Spam, spyware or adware.	Remediation handled by IT Support via JIRA ticket. **Notification:** [Organization] Management, all [Organization] Staff, As-Needed Employees and Consultants.
50 Low	A Low priority incident is unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Incident effects may be localized, but the event affects several (more than two) users or disrupts normal work for the system/LAN. Examples include a virus outbreak, local denial-of-service (DoS) attack, ransomware or non-local, emailing virus.	[Organization] CIRT and IT Support will work with vendor assets, subcontractors, consultants, hosting companies or other external entities to remediate the issue. **Notification:** [Organization] Executive Management, all The PMC Group Staff, As-Needed Employees and Consultants, where client owned systems are involved, The PMC Group system owner is notified. In case of hosted/managed system(s), hosting provider or other vendor partners are

Severity Level	NCCIC Description	[Organization] Description	Handling Procedure
			notified on a need-to-know basis.
65 Medium	A Medium priority incident may affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Incident is not localized. Involves large number of internal as well as external users. Examples include spamming Email viruses, successful hacking attempt(s), ransomware, major system shutdown, etc.	[Organization] CIRT and IT Support will work with all layers of support through to remediation, to include, state, local, and federal government. **Notification:** [Organization] Executive Management, all The PMC Group Staff, As-Needed Employees and Consultants, where client owned systems are involved, The PMC Group system owner is notified. In case of hosted/managed system(s), hosting provider or other vendor partners are notified on a need-to-know basis.
75 High	A High priority incident is likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Incident is not localized. Involves large number of internal as well as external users. Examples include spamming Email viruses, successful hacking attempt(s), ransomware, major system shutdown, etc.	[Organization] CIRT and IT Support will work with all layers of support through to remediation, to include, state, local, and federal government. **Notification:** [Organization] Executive Management, all The PMC Group Staff, As-Needed Employees and Consultants, where client owned systems are involved, The PMC Group system owner is notified. In case of hosted/managed system(s), hosting provider or other vendor partners are notified on a need-to-know basis.
90 Severe	A Severe priority incident is likely to result in a significant impact to	Incident is not localized. Involves large number of internal as well as external users. Examples	[Organization] CIRT and IT Support will work with all layers of support through to

Severity Level	NCCIC Description	[Organization] Description	Handling Procedure
	public health or safety, national security, economic security, foreign relations, or civil liberties.	include spamming Email viruses, successful hacking attempt(s), ransomware, major system shutdown, etc.	remediation, to include, state, local, and federal government. **Notification:** [Organization] Executive Management, all The PMC Group Staff, As-Needed Employees and Consultants, where client owned systems are involved, The PMC Group system owner is notified. In case of hosted/managed system(s), hosting provider or other vendor partners are notified on a need-to-know basis.
100 Emergency	An Emergency priority incident poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.	Incident is not localized. Involves large number of internal as well as external users. Examples include spamming Email viruses, successful hacking attempt(s), ransomware, major system shutdown, etc.	[Organization] CIRT and IT Support will work with all layers of support through to remediation, to include, state, local, and federal government. **Notification:** [Organization] Executive Management, all The PMC Group Staff, As-Needed Employees and Consultants, where client owned systems are involved, The PMC Group system owner is notified. In case of hosted/managed system(s), hosting provider or other vendor partners are notified on a need-to-know basis.

3.3 CYBERCOM INCIDENT HANDLING FOR DIFFERENT LEVELS OF SEVERITY

3.3.1. Cyber Severity Levels Introduction (From ACI TTP Feb 2017)

a. Description. Cyber Severity Levels are a designation of the extent to which cyber activity may impact the operational mission or supporting operational requirements.

b. Key Components

(1) CJCSM 6510.01B, Cyber Incident Handling Program, December 2014 (appendix A, section AA.15)

(2) Severity Levels

(3) Malicious Actions

CJCSM 6510.01B CYBER INCIDENT HANDLING PROGRAM/ACI TTP

CYBER SEVERITY LEVELS

I.3. Incident Severity Levels

The Severity Level Scale is a range between 3 and 0, from the least severity to the greatest severity, respectively. Table I-1 provides the ACI TTP definitions as well as the CJCSM 6510.01B definitions.

Severity Level	ACI TTP Definition	CJCSM 6510.01B Definition
Level 3 High	Has the potential to result in a demonstrable impact to the commander's mission priority, safety, or essential operations.	The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Level 2 Medium	May have the potential to undermine the commander's mission priority, safety, or essential operations.	The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Level 1 Low	Unlikely potential to impact the commander's mission priority, safety, or essential operations.	The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
Level 0 Baseline	Unsubstantiated or inconsequential event.	Not applicable.

Table I-1: Incident Severity Levels (ACI TTP)

I.4. Precedence and Category Levels

CJCSM 6510.01B provides guidance to DoD components on routine cyber events. Further, the manual states in section 1.a.(3) that in the event of emergencies and active hostilities, USCYBERCOM will provide additional guidance. The ACI TTP provides that additional guidance to ICS operators for the handling of cyber events during active hostilities or emergencies.

However, to ensure consistent reporting and integration with the cyber incident/event chain of command, the ACI TTP will characterize cyber incidences/events using the CJCSM 6510.01B Precedence and Category Levels Table (table B-A-1). This table represents the precedence and category levels located throughout the ACI TTP. The table is provided for informational purposes, as the ACI TTP characterizes cyber incidents and events within the reporting schemas.

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

Table B-A-1. Category Precedence (CJCSM 6510.01B)

I.5. Malicious Actions Table

The Malicious Actions Table (table I-3) provides actions and the resulting Severity Level.

Action	Description	Category	Severity Level
Malicious Reconnaissance	Anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability	6	2

Action	Description	Category	Severity Level
Phishing Attack	A method of causing a user with legitimate access to an information system, or information that is stored on, processed by, or transiting an information system, to unwittingly enable the defeat of a security control or exploitation of a security vulnerability	7	3
Malicious Command and Control	Method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system	7	3
Exfiltration	Information is leaked and used by an attacker	7	3
Defeating a Security Control	Compromising a physical or logical system security control	7	3
Exploitation of a Vulnerability	Something that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior	7	3
Unsuccessful Activity Attempt	Unsuccessful Logon attempts	3	2
Degradation	Performance impact; means that performance can be measured before or after event	7	3
Denial of Service (DOS)	Asset, system, or process unavailable for a period of time. A DOS within an ICS network is more serious than an external DOS attack	4	Internal-3; External-2
Modification	Data, file system, software, and/or packets were altered; set points either at rest or in transit	2	3
Injection	Introduce suspect or malicious information into a system	1	3

Action	Description	Category	Severity Level
Unauthorized Use	Resources used for attacker's own purposes; also, resources inappropriately used by a person in a position of trust	2	3

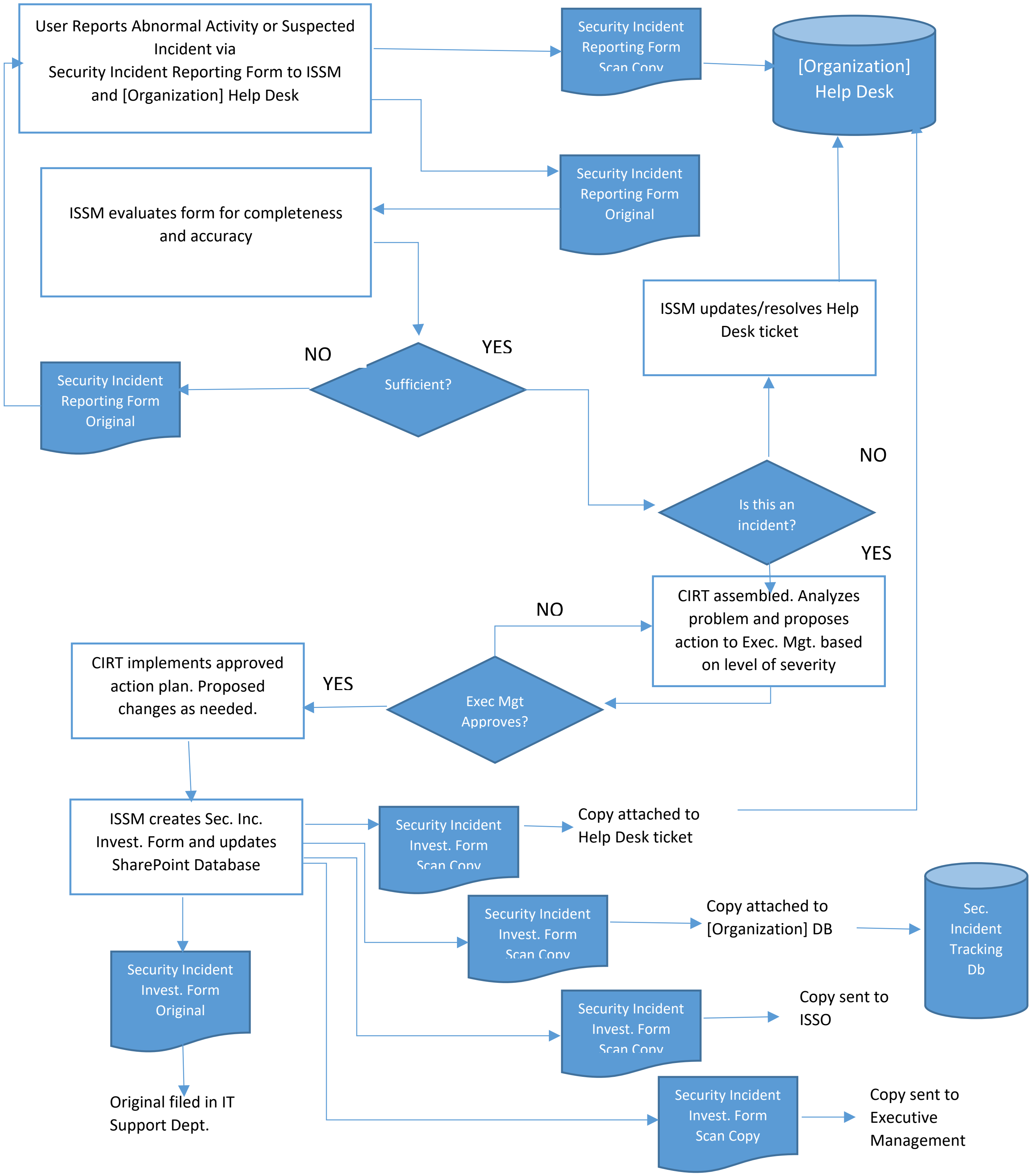
Table I-3: Malicious Actions Table (ACI TTP)

Category	Impact	Initial Notification to Next Tier	Initial Report to Next Tier	Initial submission to JIMS	Minimum Reporting
1; Root level intrusion* (Incident)	high	Within 15 minutes	Within 4 hours	Within 6 hours	Tier I
	Moderate	Within 2 hours	Within 8 hours	Within 12 hours	Tier I
	Low	Within 4 hours	Within 12 hours	Within 24 hours	Tier I
2; User level Intrusion* (incident)	high	Within 15 minutes	Within 4 hours	Within 6 hours	Tier I
	Moderate	Within 2 hours	Within 8 hours	Within 12 hours	Tier I
	Low	Within 4 hours	Within 12 hours	Within 24 hours	Tier I
3; Unsuccessful Activity Attempt	Any	Within 4 hours	Within 12 hours	Within 24 hours	Tier II
4; Denial of Service* (Incident)	high	Within 15 minutes	Within 4 hours	Within 6 hours	Tier I
	Moderate	Within 15 minutes	Within 4 hours	Within 6 hours	Tier I
	Low	As directed by CC/S/A/FA Guidance	As directed by CC/S/A/FA Guidance	As directed by CC/S/A/FA Guidance	Tier I
5; Non-Compliance Activity (Event)	All Non-Compliance Events	Within 4 hours	Within 12 hours	Within 48 hours	Tier II
6; Reconnaisance (Event)	Any	As directed by CC/S/A/FA Guidance	As directed by CC/S/A/FA Guidance	As directed by CC/S/A/FA Guidance	Tier II
7; Malicious Logic (Incident)	high	Within 15 minutes	Within 4 hours	Within 6 hours	Tier I

Category	Impact	Initial Notification to Next Tier	Initial Report to Next Tier	Initial submission to JIMS	Minimum Reporting
	Moderate	Within 2 hours	Within 8 hours	Within 12 hours	Tier II
	Low	As directed by CC/S/A/FA Guidance	As directed by CC/S/A/FA Guidance	As directed by CC/S/A/FA Guidance	Tier II
8; Investigating (Event)	N/A	Within 2 hours of notification	Consistent with the most severe possible interpretation	Within 24 hours	Tier II
9; Explained Anomaly (Event)	N/A	N/A	Within 24 hours	Within 72 hours	Tier II

Table C-A-1. Reporting Timelines (CJCSM 6510.01B)

3.4 EVENT/INCIDENT REPORTING PROCESS FLOWCHART


User Reports Abnormal Activity or Suspected Incident via
Security Incident Reporting Form to ISSM and [Organization] Help Desk
Security Incident Reporting Form Scan Copy
[Organization] Help Desk
Security Incident Reporting Form Original
ISSM evaluates form for completeness and accuracy
ISSM updates/resolves Help Desk ticket
NO
YES
Sufficient?
Security Incident Reporting Form Original
NO
Is this an incident?
YES
CIRT assembled. Analyzes problem and proposes action to Exec. Mgt. based on level of severity
NO
CIRT implements approved action plan. Proposed changes as needed.
YES
Exec Mgt Approves?
ISSM creates Sec. Inc. Invest. Form and updates SharePoint Database
Security Incident Invest. Form Scan Copy
Copy attached to Help Desk ticket
Security Incident Invest. Form Scan Copy
Copy attached to [Organization] DB
Sec. Incident Tracking Db
Security Incident Invest. Form Original
Security Incident Invest. Form Scan Copy
Copy sent to ISSO
Original filed in IT Support Dept.
Security Incident Invest. Form Scan Copy
Copy sent to Executive Management

Controlled Unclassified Information (CUI)