FACILITY-RELATED CONTROL SYSTEMS

EVENT/INCIDENT COMMUNICATION PROCEDURE (EICP)

[Replace ESTCP Logo with Organization Logo]

June 20, 2017

Organization Address

City, State, Zip Code

Controlled Unclassified Information (CUI)

Table of Contents

EXECUTIVE SUMMARY

This document supports the Event/Incident Communication Procedure for [Organization]. This Event/Incident Communication Procedure outlines the measures to consider in order for all parties to effectively communicate during a security Event/Incident incurred by [Organization]. The measures described herein include how the [Organization] Information System Security Officer (ISSO) manages the Event/Incident communication process, and identifies who they should call to report an Event/Incident, when to contact the United States Computer Emergency Readiness Team (US-CERT) for assistance, and how to ensure that all Event/Incidents are communicated to the stakeholders.

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	

Controlled Unclassified Information (CUI)

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 Events, the notification sequence for DoD, and Ransomware as a Scenario.	Michael Chipley

ABOUT THIS DOCUMENT

This document has been developed to provide guidance and procedures for [Organization] Event/Incident communications. The document was modeled after the FedRAMP template but modified to account for Events, the notification sequence for DoD, and Ransomware as a Scenario.

HOW THIS DOCUMENT IS ORGANIZED

This document is divided into six 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 communication objectives.
Section 3	Describes the Event/Incident communications roles and responsibilities.
Section 4	Describes the stakeholder communication flow process. The communication flow is described to ensure that all appropriate personnel are aware of an Event/Incident.
Section 5	Describes the life-cycle of a security Event/Incident, and what stakeholders should consider to respond effectively.
Appendix A	Describes example Event/Incident communications scenarios.

1. INTRODUCTION AND PURPOSE

Information systems are vital to [Organization] business functions; therefore, it is critical that services operate effectively without interruptions. This *Event/Incident Communication Procedure* outlines the steps for [Organization] to use when communicating information related to security Event/Incidents. The steps include the sequence of communications that should take place to ensure that all necessary information is communicated from one stakeholder to other stakeholders.

[Organization] stakeholders are those individuals and teams with a vested interest in the successful implementation and operations of [Organization] and include:

- Organization
- Stakeholders (DoD, Civilian Agencies, Nongovernmental, Commercial, Private Sector Clients)
- US-CERT
- State CERTs

The nature of unprecedented disruptions can create confusion, and often predisposes an otherwise competent IT staff towards less efficient practices. To maintain a normal level of efficiency, it is important to decrease the real-time process engineering by documenting the Event/Incident communication process prior to the occurrence of an Event/Incident. It is the goal of this *Event/Incident Communication Procedure* to ensure all appropriate stakeholders are informed of the current status of Event/Incidents, so that a full resolution is achieved in a timely manner.

1.1 APPLICABILITY

The information found in this document pertains to [Organization] information systems and data.

1.2 APPLICABLE LAWS AND REGULATIONS

The following laws and regulations are applicable to Event/Incident planning:

- Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
- Management of Federal Information Resources [OMB Circular A-130]
- Records Management by Federal Agencies [44 USC 31]
- Safeguarding Against and Responding to the Breach of Personally Identifiable Information [OMB Memo M-07-16]
- State Data Breach Laws

1.3 APPLICABLE STANDARDS AND GUIDANCE

The following standards and guidance are useful for understanding Event/Incident communication planning:

- Computer Security Event/Incident Handling Guide [NIST SP 800-61, Revision 2]
- Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]

- Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
- Risk Management Guide for Information Technology Systems [NIST SP 800-30, Revision 1]
- Payment Card Industry Standard

1.4 ASSUMPTIONS

Assumptions used in this document are as follows:

- Key personnel have been identified and are trained in their roles
- Key personnel have access to this *Event/Incident Communication Procedure*
- USCYBERCOM and US-CERT are available 24 x 7 x 365
- The affected Organization/Agency has access to the contact information for all responsible parties
- Organization/Agency *Event/Incident Response Plans* are in place and have been tested
- Organization/Agency has contractual language in place to allow sharing of relevant Event/Incident data
- Contact lists in all *Event/Incident Response Plans* are accurate and up to date
- Stakeholder contact lists have been distributed to all stakeholders.

2. OBJECTIVE

The primary objective of this document is to ensure all stakeholders communicate with each other whenever an Event/Incident occurs, allowing for a team-based approach so that Event/Incidents can be resolved quickly. Collaboration among stakeholders often results in faster resolution of the Event/Incident.

2.1 EVENTS

An event is an observable change to the normal behavior of a system, environment, process, workflow or person (components). There are three basic types of events:

- Normal—a normal event does not affect critical components or require change controls prior to the implementation of a resolution. Normal events do not require the participation of senior personnel or management notification of the event.
- Escalation – an escalated event affects critical production systems or requires that implementation of a resolution that must follow a change control process. Escalated events require the participation of senior personnel and stakeholder notification of the event.
- Emergency – an emergency is an event which may impact the health or safety of human beings breach primary controls of critical systems materially affect component performance or because of impact to component systems prevent activities which protect or may affect the health or safety of individuals be deemed an emergency as a matter of policy or by declaration by the available incident coordinator

Computer security and information technology personnel must handle emergency events according to well-defined computer security incident response plan.

2.2 INCIDENT

An incident is an event attributable to a human root cause. This distinction is particularly important when the event is the product of malicious intent to do harm. An important note: all incidents are events but many events are not incidents. A system or application failure due to age or defect may be an emergency event but a random flaw or failure is not an incident.

2.3 COMPUTER INCIDENT RESPONSE TEAM (CIRT)

The incident coordinator manages the response process and is responsible for assembling the team. The coordinator will ensure the team includes all the individual's necessary to properly assess the incident and make decisions regarding the proper course of action. The incident team meets regularly to review status reports and to authorize specific remedies. The team should utilize a pre-allocated physical and virtual meeting place.

2.4 INCIDENT INVESTIGATION

The investigation seeks to determine the circumstances of the incident. ***Every incident will warrant or require an investigation.*** However, investigation resources like forensic tools, dirty networks, quarantine networks and consultation with law enforcement may be useful for the effective and rapid resolution of an emergency incident.

3. ROLES AND RESPONSIBILITIES

The [Organization] ISSO has oversight responsibility for ensuring appropriate communications occurs for all reported outages, disruptions, and Event/Incidents for [Organization] systems. [Organization] ISSOs are trained in their duties, and ensure all appropriate parties are made aware of the status of Event/Incidents.

All Event/Incidents have the notion of *first respons*e. A *first responder* is the individual who first brings the Event/Incident (or suspected Event/Incident) to the attention of others. A first responder can be any type of user (e.g. a system administrator, a customer) or a monitoring center. In the case of [Organization], a first responder could be a staff member, a customer, USCYBERCOM, or US-CERT.

Working as a team, [Organization] ISSO, customers, USCYBERCOM, and the US-CERT are positioned to handle and resolve Event/Incidents faster through collaborative methods than if each entity worked on the Event/Incidents alone.

FISMA §3546 requires that US-CERT: *Provide timely technical assistance to operators of agency information systems regarding security Event/Incidents, including guidance on detecting and handling information security Event/Incidents.*

If [Organization] will require additional assistance in Event/Incident resolution, they will need to communicate this need to DoD and possibly US-CERT. [Organization] understands that asking for additional Event/Incident support, and resolving the Event/Incident quickly, will have fewer

repercussions on customers systems, and on their Provisional Authorization, than refusing assistance and leaving the Event/Incident unresolved for a much longer period of time.

Note: The US-CERT website can be found at the following URL:
http://www.us-cert.gov

The following sections outline the roles and responsibilities for the various stakeholders in the Event/Incident communication process.

3.1 [ORGANIZATION] ISSO

The [Organization] ISSO is headquartered at the main office of [Organization] and provides oversight for Event/Incidents.

[Organization] ISSO can be a first responder and is also dependent on after action reports from other stakeholders. The role of [Organization] ISSOs in the Event/Incident communication process is described below.

- Records all Event/Incident communications in the [Organization] database
- Ensures that the appropriate stakeholders are kept updated
- Monitors the communication flow between stakeholders
- Ensures timely closure of all Event/Incidents
- Ensures that POAMs are created if needed as a result of an Event/Incident
- Discusses with Legal and Insurance the option of requesting outside assistance (e.g. 3rd Party Forensics, USCYBERCOM, or US-CERT)
- Makes use of after action reports to facilitate further communications
- In the event of a major Event/Incident affecting multiple customers, escalates and facilitates communications to [Organization] Executives, DoD, and others as necessary.

Note: At this time, [Organization] ISSOs are available during regular business hours, Eastern time. After hours contact information is provided in the Information System Contingency Plan (ISCP).

3.2 ORGANIZATIONS

Organizations should report all Event/Incidents consistent with the organization's Event/Incident response policy. Each organization should designate a primary and secondary POC for Event/Incident communications. Organization POCs should be shared with the [Organization] ISSO, DoD, and possibly US-CERT. Organizations general responsibilities are described below.

- Notify ESTCP if the organization becomes aware of an Event/Incident that [Organization] has not yet identified or reported
- Provide a primary and secondary POC for [Organization], DoD, and US-CERT as described in organization and [Organization] *Event/Incident Response Plans*
- Work with ESTCP to resolve Event/Incidents; provide coordination with DoD and US-CERT if necessary
- Monitor security controls that are organization responsibilities.

3.4 US-CERT

FISMA requires federal agencies to report Event/Incidents US-CERT acts as the government wide Event/Incident response organization that assists civilian federal agencies in their Event/Incident handling efforts. US-CERT does not replace any existing agency response teams; rather, it augments the efforts of the federal civilian agencies by serving as a focal point when dealing with Event/Incidents. The responsibilities of US-CERT are outlined in 44 U.S.C. § 3546 and are summarized as follows:

- Notify agency POCs and [Organization] ISSO of known Event/Incidents
- Coordinate cyber security operations and Event/Incident response
- Monitor and report security Event/Incidents and network flow data
- Distribute advisories on potential threats
- Assists government-wide and agency-specific efforts to provide adequate, risk- based and cost-effective cyber security.

Separate procedures are in place for the Department of Defense as identified in Directive O-8530-1 and all components report Event/Incidents to the Joint Task Force Global Network Operations (JTF-GNO), which, in turn, coordinates directly with the US-CERT.

4. STAKEHOLDER COMMUNICATIONS

The following sections outline communications recommendations based on the different first responder possibilities. A first responder must have the ability to notice or detect events on the system.

The path of Event/Incident communications will be different based on who happens to be the first responder. There are two scenarios an organization must consider: first an Event/Incident that occurs to the Corporate IT systems (accounting, email, HR, etc.) that could expose company sensitive/proprietary data and/or information; and secondly, an Event/Incident that exposes ESTCP Project Controlled Unclassified Information (CUI). Corporate IT Systems typically have Insurance and Legal reporting requirements and possibly notification to US-CERT and State-CERTS if Personally Identifiable Information (PII), Payment Card Information (PCI), or other sensitive data has been exposed. ESTCP Project data reporting requirements are dictated by DoDI's 8500/8510 and are reported through the USCYBERCOM reporting process.

4.1 [ORGANIZATION] IS THE FIRST RESPONDER, ONE OR MORE OTHER ORGANIZATIONS AFFECTED

If [Organization] detects an Event/Incident that has the potential to cause an organization service availability disruption, a compromise of data confidentiality, or a compromise of organizational data integrity, [Organization] will notify ESTCP, and if required, their Legal and Insurance, and proceed to have a 3rd party forensics investigation (USCYBERCOM or Private Sector firm) to confirm an event is an incident.

[Organization] will proceed with notification to stakeholders in accordance with its Event/Incident Response Plan. [Organization] will first notify the stakeholders who have the potential to be affected by the Event/Incident. All organizations that receive [Organization]

Event/Incident reports should inform [Organization] if they plan on asking for assistance from USCYBERCOM or US-CERT. If the organization opts to request assistance from USCYBERCOM or US-CERT, the organization should notify US-CERT and provide US-CERT with information on the [Organization] ISSO.

The [Organization] ISSO will record information related to the Event/Incident in the [Organization] database, and will monitor next steps. The process that should be used when [Organization] is a first responder is illustrated in Figure 4-1.

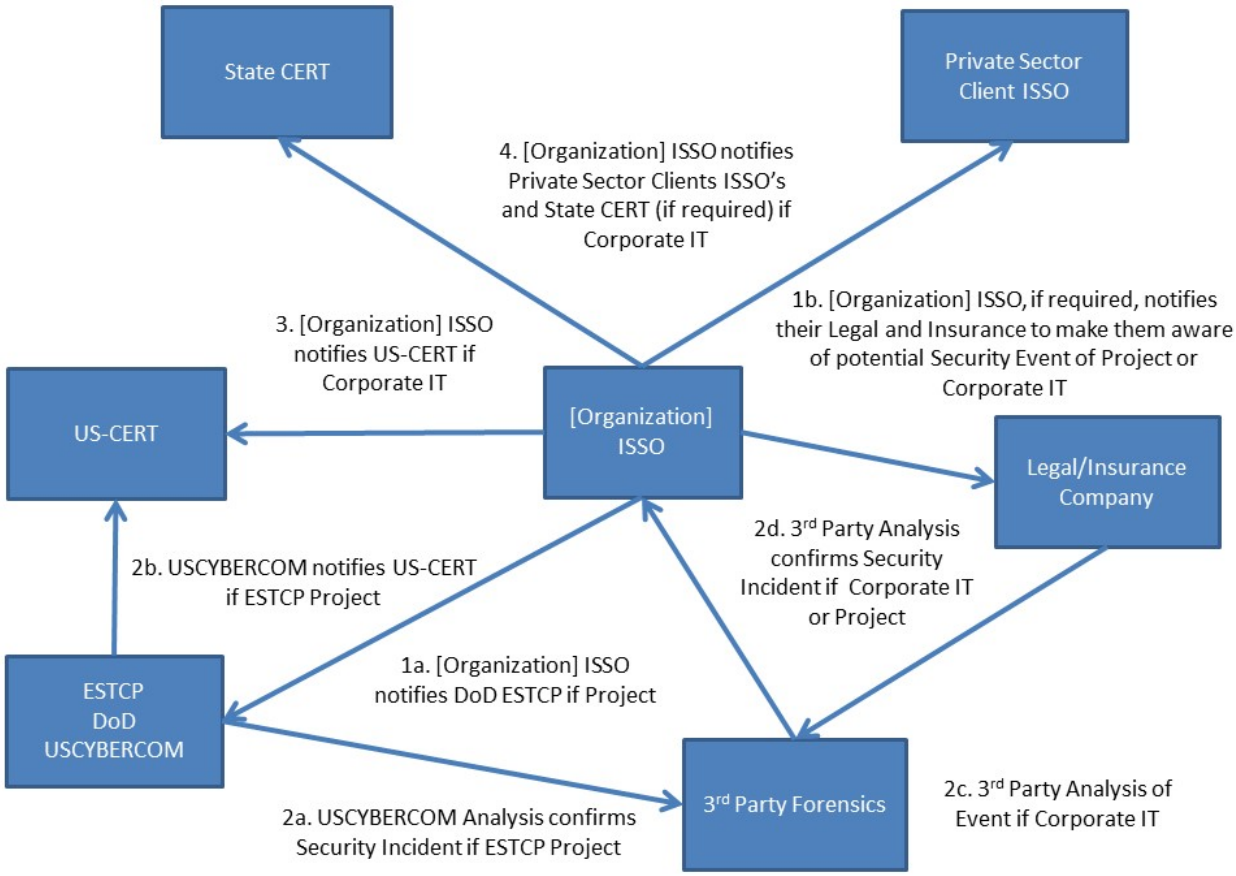

Figure 4-1. [Organization] is the First Responder, Event/Incident Affects One or More Other Organizations

4.2 DOD ORGANIZATION IS THE FIRST RESPONDER

It is possible that a DoD organization (Services, Agencies, Cloud Service Provider, etc.) may become suspicious of activity they are seeing on the Joint Information Environment (JIE) before it is evident at the HBSS/ACAS monitoring center. An Event/Incident on an DoD organization host sitting on a cloud system, completely local to the organization host, might be unrelated to anything happening below the hypervisor on the underlying cloud infrastructure. DoD Organizations will want to confirm with [Organization] whether that is the case or not.

Organizations should take into consideration that Event/Incidents could occur on virtual machines due to reasons unrelated to the underlying cloud architecture.

When an DoD Organization is the first responder, it will notify ESTCP of the suspicious activity or Event/Incident who will notify the [Organization] ISSO. DoD Organizations will work with the [Organization] to determine if the Event/Incident is local to the organization host (or hosts), or is part of a larger Event/Incident that affects DoD's underlying JIE and cloud infrastructure – affecting multiple cloud tenants. After communications with [Organization] takes place, the DoD Organization ISSO will contact USCYBERCOM who will contact US-CERT to confirm that US-CERT has been made aware of the Event/Incident. [Organization] ISSO will engage in a dialogue with DoD Organization to obtain all relevant information. The [Organization] may need to enlist the support of US-CERT according to the organization security policies and Event/Incident Response Plan.

The [Organization] ISSO will record information related to the Event/Incident in the [Organization] database, and will monitor next steps. The process that should be used when the DoD Organization is the first responder is illustrated in Figures 4-2.

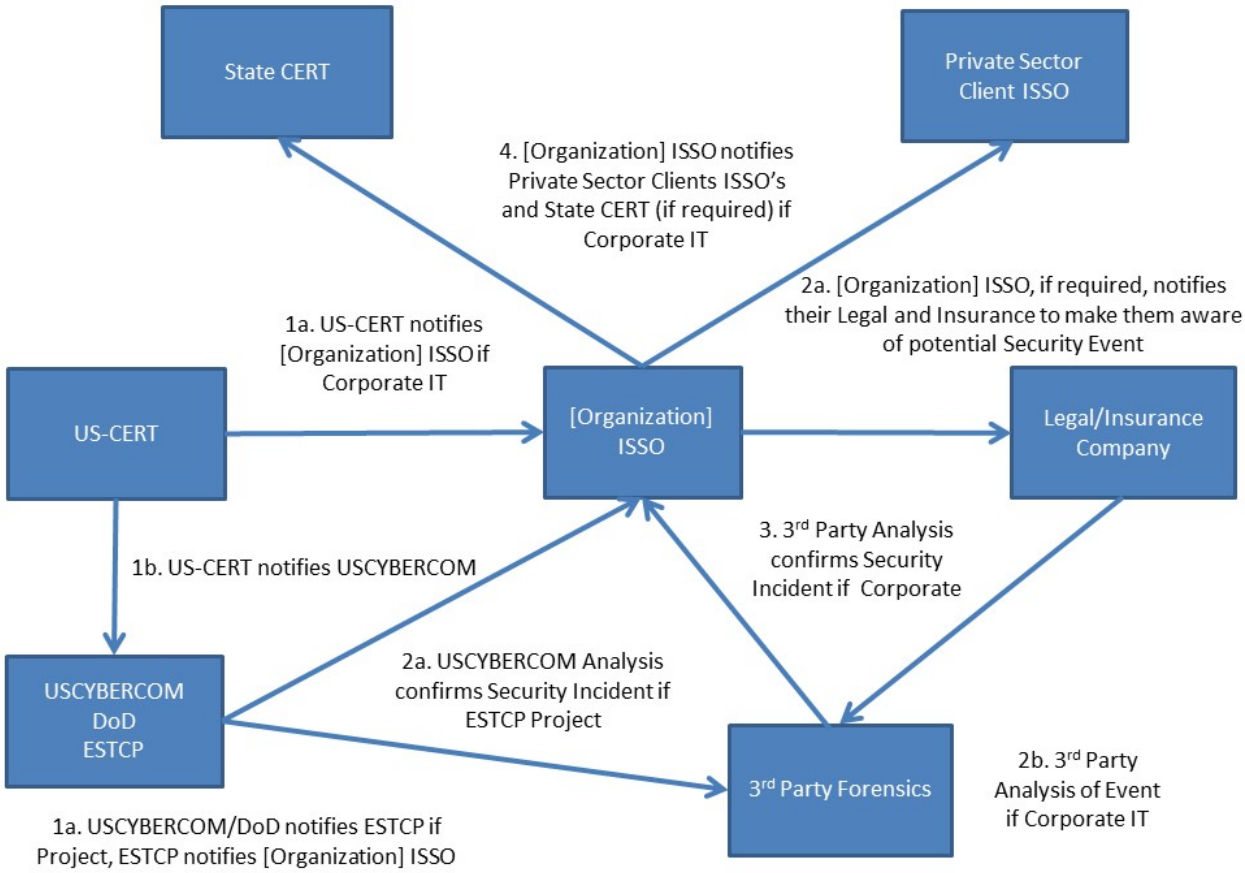

Figure 4-2a. DoD Organization is the First Responder

4.3 US-CERT IS THE FIRST RESPONDER

In certain circumstances, US-CERT may become aware of potential or real Event/Incidents before it has become evident to [Organization] or the organization. US-CERT captures network flow data via sensors that enable them to correlate and identify malicious activity. Network anomalies discovered on traffic that traverses Trusted Internet Connections (TICs) is another mechanism that US-CERT uses to become aware of Event/Incidents. Additionally, US-CERT serves as a general Event/Incident response center for the U.S. government and the U.S. private sector, and as a result, often becomes aware of Event/Incidents sooner than other entities. US-CERT may want to bring malicious activity to the attention of organizations. When US-CERT is the first responder, it will notify affected organizations of the suspicious activity or Event/Incident. US-CERT should work with the organization to determine if the Event/Incident is local to the organization, or is part of a larger Event/Incident that affects multiple organizations, and their underlying cloud infrastructures.

Working with the organization, US-CERT should ascertain whether the Event/Incident appears to affect [Organization]. If [Organization] appears to be affected, US-CERT then notifies the [Organization] ISSO. The process that should be used when US-CERT is the first responder is illustrated in Figure 4-3.

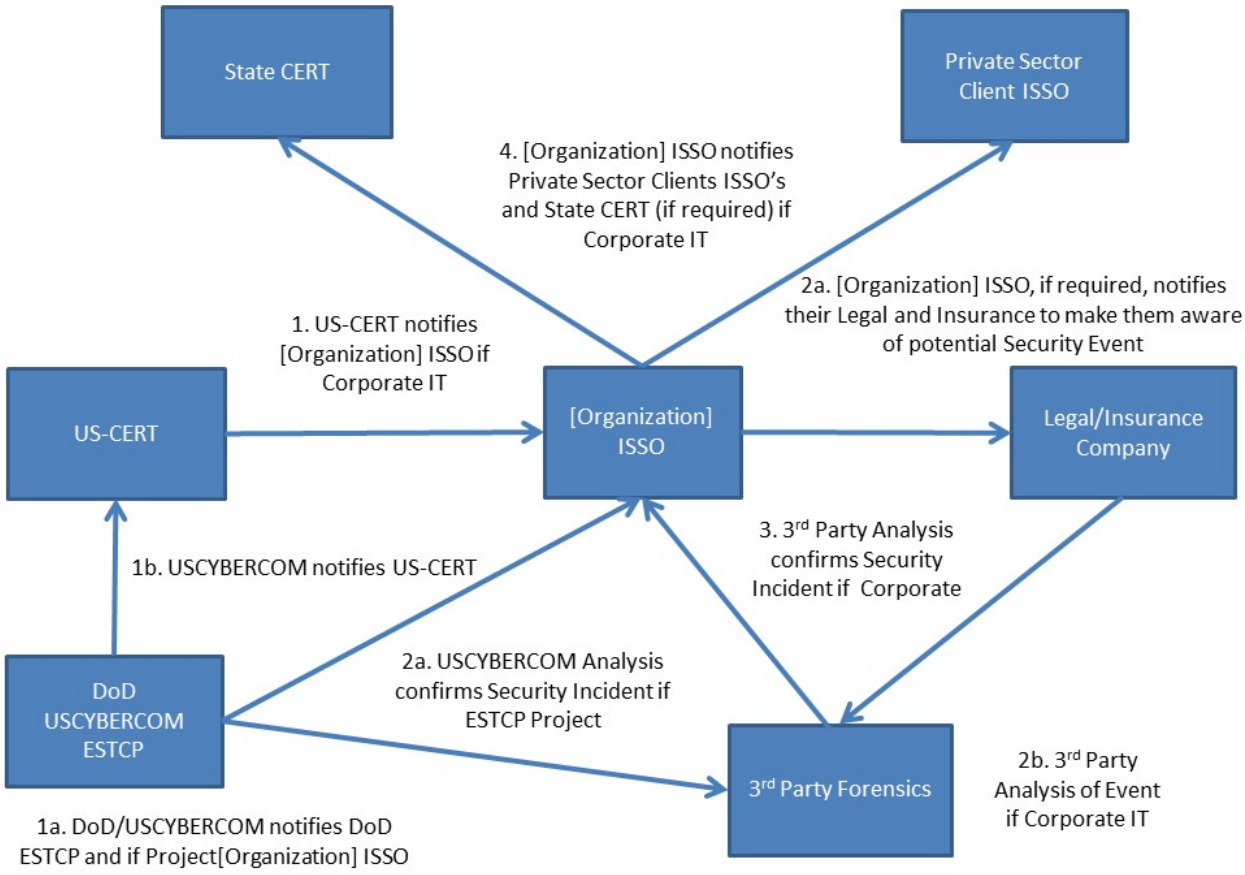

Figure 4-3. US-CERT is the First Responder

Various Event/Incident response scenarios are illustrated in Appendix A.

5. THE SECURITY EVENT/INCIDENT LIFE-CYCLE

The Security Event/Incident Life-Cycle, illustrated in Figure 5-1, is composed of the following phases: Preparation, Detection and Analysis, Containment and Eradication, Recovery, and the Post-Event/Incident Activities.

Figure 5-1. Event/Incident Life-Cycle

Some of the life-cycle activities are performed in parallel with each other (e.g. analysis, communication and documentation).

- **Preparation**: Maintaining and improving the first responder's Event/Incident response capabilities;
- **Detection and Analysis**: Detection, confirmation, and analysis of suspected Event/Incidents;
- **Containment & Eradication**: Minimizing loss, theft of information, or disruption of service, and elimination of the threat;
- **Recovery:** Restoring the computing services securely and in a timely manner;
- **Post-Event/Incident Activity**: Assessment of the Event/Incident response to better handle future Event/Incidents through the utilization of logs review, "Lessons Learned" and after-action reports, or the mitigation of exploited vulnerabilities to prevent similar Event/Incidents in the future.

In addition to the above listed activities, there are various cross-cutting elements which are always present throughout the Security Event/Incident Life-Cycle:

- **Communication:** The [Organization]ISSO must ensure that all stakeholders are notified as appropriate. Each stakeholder should have information that is consistent with other stakeholders.
- **Analysis:** All stakeholders should perform continuous examination of available data to support decision-making throughout the security Event/Incident life-cycle.
- **Documentation:** All stakeholders should record and time-stamp status information and any evidence obtained from detection through post-Event/Incident activity. If a forensic investigation is being performed chain of custody should be recorded.

5.1 PREPARATION

When preparing for an Event/Incident, stakeholders should take into consideration the following questions:

1. What preparations have been made by the Event/Incident response team?
2. Has the Event/Incident Response Plan been tested?
3. Are former Lessons Learned archived where all team members can access them?
4. Is the contact list in the Event/Incident Response Plan up to date?
5. Does staff listed in the Event/Incident Response Plan contact list have a copy of the plan?
6. What were past precursors of Event/Incidents?
7. What tools are available in house to perform Event/Incident handling?

5.2 DETECTION AND ANALYSIS

There are certain types of system and network activities that are often considered suspicious. Not all suspicious activity constitutes a security Event/Incident and should therefore be carefully researched and analyzed before any decisions are made.
When trying to determine if an Event/Incident has in fact taken place and what items require analysis, stakeholders should take into consideration the following questions:

1. What indicators caused someone to think that an Event/Incident might have occurred?
2. When did the problem start and is it still on-going?
3. Where did the suspicious activity take place? What servers and networks?

5.3 CONTAINMENT, ERADICATION, AND RECOVERY

Containing an Event/Incident means not letting it spread further to other systems and networks. Eradication refers to removing it completely. When handling an Event/Incident, initially, priority should always be given to containment. There may be reasons why eradicating an Event/Incident is not initially the right course of action. For example, if you eradicate the Event/Incident before performing forensics, you may not be able to identify the cause of the Event/Incident, or the perpetrator. If you want to perform memory forensics on a server, you

cannot shut the server down, otherwise you clear out the memory on the server and you are left with nothing to analyze.

Decisions need to be made before an Event/Incident is eradicated on whether it is best to simply recover quickly, or perform advanced forensics. If the plan is to perform a forensic investigation for the purpose of identifying a perpetrator for prosecution, evidence needs to be preserved. If the Event/Incident is eradicated before evidence is preserved, then it is not possible to perform a forensic investigation.

When performing containment, eradication, and recovery, stakeholders should take into consideration the following questions:

1. What strategy should the organization take to contain the Event/Incident?
2. What could happen if the Event/Incident were not contained?
3. What additional tools might be needed to respond to this particular Event/Incident?
4. What sources of evidence, if any, should the organization acquire?
5. How should the evidence be acquired?
6. Where will the evidence be stored?
7. How long should evidence be retained?
8. Which team members should be involved in the containment, eradication, and/or recovery processes?

5.4 POST-EVENT/INCIDENT ACTIVITY:

Post-Event/Incident activity refers to reviewing and reflecting on the recently closed Event/Incident for the purpose of preventing such Event/Incidents from occurring in the future.

When performing post-Event/Incident activities, stakeholders should take into consideration the following questions:

1. Who should attend the post-Event/Incident lessons learned meetings regarding this Event/Incident?
2. What could be done to prevent similar Event/Incidents from occurring in the future?
3. What could be done to improve the detection of similar Event/Incidents?
4. How many Event/Incident response team members participated in handling this Event/Incident?
5. Did we have the right people participating on the team?
6. How long did it take to close the Event/Incident once it was identified?
7. Besides the Event/Incident response team, what groups within the [Organization] were involved in handling and eradicating this Event/Incident?
8. What tools and resources did the team use in handling this Event/Incident?

9. What aspects of the handling might have been different if the Event/Incident had occurred at a different day and time (on-hours versus off-hours)?

10. What aspects of the handling might have been different if the Event/Incident had occurred at a different physical location (primary versus alternate site)?

APPENDIX A: EVENT/INCIDENT RESPONSE SCENARIOS

The National Institute of Standards and Technology (NIST) *SP 800-61, Revision 2, Computer Security Event/Incident Handling Guide*, provides various scenarios as an effective way to help organizations build their Event/Incident response skills and identify potential issues with their Event/Incident response processes. [Organization]has created the following scenarios and questions with the recommended responses, so that each [Organization]stakeholder can better understand their role during a security Event/Incident.

Each scenario below is followed by Event/Incident-specific questions and suggested responses. [Organization]stakeholders are encouraged to adapt these scenarios and questions for use in their own Event/Incident response exercises. Note that the responses presented in these scenarios are for guidance only and in most cases will not represent the full communications dialogue in its entirety. The illustrative scenarios presented present only a subset of the communications required for each Event/Incident.

A.1 SCENARIO 1: DOMAIN NAME SYSTEM (DNS) SERVER DENIAL OF SERVICE (DOS)

On a Saturday afternoon, external users start having problems accessing an agency's public websites. Over the next hour, the problem worsens to the point where nearly every access attempt fails. Meanwhile, a staff member of [Organization]'s networking staff responds to alerts from an Internet border router and determines that the organization's Internet bandwidth is being consumed by an unusually large volume of User Datagram Protocol (UDP) packets to and from both of the [Organization]'s public DNS servers. Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address. Also, all the DNS requests from that address come from the same source port.

[ORGANIZATION] SHOULD CONSIDER THE FOLLOWING KEY QUESTIONS:

1. Who should [Organization] contact for more information on the external IP address in question?
2. Suppose that after the initial containment measures were put in place, the network administrators detected that nine internal hosts were also attempting the same unusual requests to the DNS server. How would that affect the handling of this Event/Incident?
3. Suppose that two of the nine internal hosts disconnected from the network before their system owners were identified. How would the system owners be identified?

RECOMMENDED RESPONSES

1. [Organization] should contact their ISP for assistance. The customer organization should offer [Organization] assistance from US-CERT and should contact US-CERT and provide to them the [Organization] POC so that US-CERT can reach out to [Organization].
2. The nine internal hosts should be taken off the network and scanned for malware. If none is found, but the problem still exists, [Organization] should consider reimaging the hosts.

3. [Organization] should review the log files on their DNS servers, routers, and firewalls to identify the two hosts.

A.2 SCENARIO 2: COMPROMISED DATABASE SERVER

On a Tuesday night, a [Organization] database administrator performs some off-hours maintenance on several production database servers. The administrator detects some unfamiliar and unusual directory names on one of the servers. After reviewing the directory listings and viewing some of the files, the administrator concludes that the server has been attacked and calls the Event/Incident response team for assistance. The team's investigation determines that the attacker successfully gained root access to the server six weeks ago.

[ORGANIZATION] SHOULD CONSIDER THE FOLLOWING KEY QUESTIONS:

1. What sources might the team use to determine when the compromise had occurred?
2. How would the handling of this Event/Incident change if the team found that the database server had been running a packet sniffer and capturing passwords from the network?
3. How would the handling of this Event/Incident change if the team found that the server was running a process that would copy a database containing sensitive customer information (including personally identifiable information) each night and transfer it to an external address?
4. How would the handling of this Event/Incident change if the team discovered a rootkit on the server?

RECOMMENDED RESPONSES

1. The Event/Incident response team should review the system's log files.
2. All system passwords on the network should be changed immediately.
3. The external address should be blocked (blacklisted) and the database log files should be reviewed to determine if sensitive information has been compromised. [Organization] should notify the affected customers immediately.
4. [Organization] should ask their agency POC to request help from US-CERT, as this may have a wide-spread impact on federal customers.

A.3 SCENARIO 3: WORM AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK

On a Tuesday morning, a new worm is released; it spreads itself through removable media, and it can copy itself to open Windows shares. When the worm infects a host, it installs a DDoS agent. In the past, [Organization] incurred widespread infections before antivirus signatures became available several hours after the worm started to spread.

[ORGANIZATION] SHOULD CONSIDER THE FOLLOWING KEY QUESTIONS:

1. How should [Organization] Event/Incident response team identify all infected hosts?
2. How should [Organization] attempt to prevent the worm from entering the system before antivirus signatures are released?

3. How should [Organization] attempt to prevent the worm from potentially spreading before antivirus signatures were released?

4. Should [Organization] attempt to patch all vulnerable machines? If so, how is this be performed?

5. How should the handling of this Event/Incident change if infected hosts (that had received the DDoS agent) had been configured to attack another entity's website the next morning?

6. How should the handling of this Event/Incident change if one or more of the infected hosts contained personally identifiable information?

7. How should the Event/Incident response team keep agency customers informed about the status of the Event/Incident?

8. What additional measures should [Organization] team perform for hosts that are not currently connected to the network (e.g., staff on vacation that currently do not have their laptops connected to the network)?

RECOMMENDED RESPONSES

1. The worm, after infecting a host, will try to scan neighboring IP addresses to find the next targets. Neighboring IP addresses can be a good place to detect if a host is infected with a worm. Generally, any legitimate program runs on a specific location on a network. Worms, on the other hand, need to find targets. If we monitor the number of IP addresses scanned by the host, and if it exceeds a certain threshold, then we can safely assume that a worm has been detected.

2. [Organization] should make use of reputable Intrusion Prevention and Antivirus tools on all systems within the security boundary.

3. [Organization] should aggressively quarantine any process that shows erratic behavior. After isolating the process, it should be monitored for a period of time corresponding to the erratic behavior shown by the process. If the process does not show any aberrant behavior during the time it's monitored, it can be released. If it shows the same behavior again and again, it is quarantined and labeled as a worm.

4. [Organization] should have an active patch and update program in place, and should use the change management process documented in their Configuration Management Plan.

5. All agencies connected to [Organization] should be made aware of the infestation, so that their Event/Incident response teams can activate to assess their systems and take remedial actions, if needed.

6. System log files should be reviewed to determine if any sensitive information has been compromised. [Organization] should notify any affected customers immediately.

7. [Organization]'s Event/Incident response team should work with the [Organization] ISSO to ensure all affected parties are notified.

8. Hosts not currently on the network, should be identified and scanned before being allowed to connect to the network.

A.4 SCENARIO 4: RANSOMWARE ATTACK

On a Tuesday morning, a Ransomware attack occurs that encrypts IT systems files and databases, and requires Bitcoin payment to restore the files and data. The AV/Malware application was not able to stop the ransomware before it was able to encrypt one organizations Enclave/DMZ. [Organization] System Administrators were able to isolate the

infected/exploited servers and prevent the ransomware from hopping to the other Enclaves/DMZ's.

[ORGANIZATION] SHOULD CONSIDER THE FOLLOWING KEY QUESTIONS:

1. How should [Organization] Event/Incident response team identify all infected hosts?
2. How should [Organization] attempt to prevent the ransomware from entering the system before antivirus signatures are released?
3. How should [Organization] attempt to prevent the worm from potentially spreading before antivirus signatures were released?
4. Should [Organization] attempt to patch all vulnerable machines? If so, how is this be performed?
5. How should the handling of this Event/Incident change if infected hosts (that had received the ransomware) had been configured to attack another entity's website the next morning?
6. How should the handling of this Event/Incident change if one or more of the infected hosts contained personally identifiable information?
7. How should the Event/Incident response team keep agency customers informed about the status of the Event/Incident?
8. What additional measures should [Organization] team perform for hosts that are not currently connected to the network (e.g., staff on vacation that currently do not have their laptops connected to the network)?

RECOMMENDED RESPONSES

1. The randomware, after infecting a host, will try to scan neighboring IP addresses to find the next targets. Neighboring IP addresses can be a good place to detect if a host is infected with ransomware.
2. [Organization] should make use of reputable Intrusion Prevention and Antivirus tools on all systems within the security boundary.
3. [Organization] should aggressively quarantine any process that shows erratic behavior. After isolating the process, it should be monitored for a period of time corresponding to the erratic behavior shown by the process. If the process does not show any aberrant behavior during the time it's monitored, it can be released. If it shows the same behavior again and again, it is quarantined and labeled as rannsomware.
4. [Organization] should have an active patch and update program in place, and should use the change management process documented in their Configuration Management Plan.
5. All agencies connected to [Organization] should be made aware of the infestation, so that their Event/Incident response teams can activate to assess their systems and take remedial actions, if needed.
6. System log files should be reviewed to determine if any sensitive information has been compromised. [Organization] should notify any affected customers immediately.
7. [Organization]'s Event/Incident response team should work with the [Organization] ISSO to ensure all affected parties are notified.
8. Hosts not currently on the network, should be identified and scanned before being allowed to connect to the net