CENTERS for MEDICARE & MEDICAID SERVICES
Enterprise Information Security Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Enterprise Information Security Group

Risk Management, Oversight, And Monitoring

Risk Management Handbook
Volume II
Procedure 7.2
Incident Handling

FINAL
Version 1.0
December 6, 2012

Document Number: CMS-CISO-2012-vII-pr7.2

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *INCIDENT HANDLING,* VERSION 1.0

1. Baseline Version. This document, along with its corresponding *Risk Management Handbook (RMH)*, Volume III Standard, replaces *CMS Information Security (IS) Incident Handling and Breach Analysis/Notification Procedure*, dated December 3, 2010.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

(This Page Intentionally Blank)

1 OVERVIEW

1.1 PURPOSE

The purpose of this procedure is to provide an inclusive set of procedures for responding to an identified *security* or *privacy* incident. These procedures should be used by ANY CMS employee or contractor to report an incident, or suspected incident to the proper CMS authorities. This procedure also provides inter- and intra- CMS operating procedures for managing the internal response to suspected or actual security or privacy incidents.

Users of these procedures include CMS system users (contractor or federal employees), CMS Information System Security Officers (ISSOs), Business Partner or contractor System Security Officers (SSOs), CMS Computer Security Incident Response Team (CSIRT) personnel, CMS Security Operations Center (SOC) personnel, or other applicable CMS or CMS-contractor personnel.

CMS contractors or other relevant CMS organizations *may* supplant these procedures with internal (corporate) procedures, *provided* those procedures interface appropriately with the applicable CMS processes and procedures contained herein. For questions regarding this procedure, contact the CMS Enterprise Information Security Group (EISG) at Mailto:CISO@CMS.hhs.gov.

This *Risk Management Handbook (RMH)* Volume II, Procedure 7.2, *Incident Handling*, along with the companion Volume III, Standard 7.1, *Incident Handling and Breach Notification*, supersedes the *CMS Information Security (IS) Incident Handling and Breach Analysis/Notification Procedure* dated December 3, 2010.

1.2 RELATED DOCUMENTATION

A more detailed description of the elements necessary to have an effective security and privacy incident response capability is described in the RMH Volume III, Standard 7.1, *Incident Handling and Breach Notification*. RMH Volume III, Standard 7.1 describes and defines the elements associated with an *"incident"*, the elements of an effective incident response *capability*, and the *Roles and Responsibilities* associated with the CMS incident response program. It is necessary to have a basic understanding of those elements in order to perform some of the specific security functions detailed in this procedure.

The RMH Volume III, Standard 7.1, *Incident Handling and Breach Notification* provides detailed definitions and high-level guidance on security events and incidents, privacy incidents, and the different types of information and scenarios involved. A basic understanding of these terms is required in order to fully understand and implement *some* of the following procedures, with the exception of the *Initial Incident Reporting* procedure.

2 PROCEDURE

PROCEDURE	PRINCIPLE
2.1 INCIDENT HANDLING	
2.1.1 INITIAL INCIDENT REPORTING	
2.1.1.1 PROCEDURE USERS	
1. CMS Information System Security Officer (ISSO).	
2. Business Partner System Security Officer (SSO).	
3. System Users.	*CMS employees or contractor staff conducting CMS business functions.*
4. CMS CSIRT personnel.	
5. CMS SOC personnel.	
6. On-site Incident Response (IR) authority.	
7. Other applicable IR personnel.	
2.1.1.2 ENTRY CONDITIONS	
1. A *Security Incident, Reportable Event,* or data *Breach* is believed, or suspected, to have occurred.	*If the conditions are such that it cannot be determined whether a security incident, reportable event, breach, or privacy incident has actually occurred, then as a precaution, the activity or occurrence should be reported so that additional response resources can be mobilized to determine the extent of the issue.*

PROCEDURE	PRINCIPLE
2.1.1.3 INITIAL REPORTING PROCEDURE	
1. If the incident has occurred at a CMS contractor *hosted* or *managed* site:	
a. Report to the *On-site Incident Response (IR) Authority.*	*CMS contractors are responsible for establishing and maintaining an organizational incident response (IR) capability. (See* CMS Acceptable Risk Safeguards (ARS)*, IR family of control requirements available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.)*
NOTE: **The timeliness requirements for reporting incidents will be dependent on the category of the incident (see Figure 1) and the type of information involved. If the extent of the incident is not fully understood, DO NOT DELAY reporting of the incident.**	
2. Report the incident to ***CMS***. Be prepared to provide the following information:	QualityNet *users call* QualityNet Help Desk *at (866) 288-8912 and/or email qnetsupport@sdps.org; ALL others (or if in doubt) contact the* CMS IT Service Desk *at (410) 786-2580 and/or email CMS_IT_Service@cms.hhs.gov.*
a. Name, phone number (primary and secondary), and email address of the *Point-Of-Contact* (POC) at the reporting site.	*This person will be contacted by the* CMS Security Incident Response Team (CSIRT) *for immediate follow-up on the specifics of the incident.* *If required, the POC may be updated to be the* On-site Incident Response Authority *later in the IR process.*

PROCEDURE	PRINCIPLE
b. A description of the incident, including:	*Additional detail of the desired information can be found in the CMS* Computer Security Incident Report *(CSIR).*
(1) The *initial* assessment of the *Incident Category* as defined in Figure 1.	*Note that timeliness requirements for reporting may also be driven by the applicable incident category.*
(2) The affected location and/or named system.	*This information is important for establishing the applicable Business Owner POC.*
(3) The date and time (including time zone) that the incident occurred.	
(4) If the incident involves, or may involve, *Personally Identifiable Information* (PII), also provide the following:	*In addition to PII as defined by the* Privacy Act of 1974, *PII may also include information defined as* Protected Health Information *(PHI) and/or* Federal Tax Information *(FTI).*
(a) Estimated number of individuals, and/or records, affected.	
(b) The type of PII involved, including (if possible) the specified data fields involved.	*Data fields may include name, SSN, diagnoses, address, phone number, or other attributes that might be used to individually identify the affected persons.*
(5) If any *Law Enforcement* organization has been mobilized.	
NOTE: **Do NOT delay initial reporting in order to gather the information requested in Step (6) below. This information may be provided later, as determined by the CMS CSIRT.**	*It may be researched and reported as part of the Response phase of the incident handling process.*
(6) If available and applicable, also report:	
(a) Source IP, port, and protocol.	
(b) Destination IP, port, and protocol.	
(c) Operating System (including version, patches, etc.)	

PROCEDURE	PRINCIPLE
(d) System function (e.g., DNS/ web server, workstation, etc.) (e) Antivirus software installed, including version, and latest updates. (f) Method used to identify the incident (e.g., IDS, audit log analysis, system administrator.) 3. If the incident has occurred at a contractor *hosted* or *managed* site: a. Coordinate subsequent actions through the contractor *on-site IR authority*. 4. Coordinate with the CMS CSIRT for immediate response, recovery, and follow-up actions. 5. On-site IR authorities proceed to *On-Site Response*, Section 2.1.2.	
2.1.2 ON-SITE RESPONSE	
2.1.2.1 PROCEDURE USERS	
1. On-site incident response authority personnel/staff.	*After initial reporting of an incident, the* on-site IR authority *performs these actions.*
2.1.2.2 ENTRY CONDITIONS	*This procedure is applicable if ANY of these* Entry Conditions *exist.*
1. A *Security/Privacy Incident, Reportable Event*, or *Data Breach* is believed, or suspected, to have occurred. 2. The *Incident, Reportable Event*, or *Data Breach* has been reported to the on-site IR authority. 3. The *Incident, Reportable Event*, or *Data Breach* has been reported to CMS.	

PROCEDURE	PRINCIPLE
2.1.2.3 ON-SITE RESPONSE PROCEDURE	
1. Establish communications with the *CMS CSIRT* to coordinate further actions.	*This does not mandate a continuous uninterrupted communications link. The* on-site IR authority *need only ensure consistent and reliable POCs, with reliable methods, are identified and instituted.*
2. Prepare an *initial* written *Incident Report* and submit to the CMS CSIRT in accordance with Section 2.1.19.	
3. If direct *RiskVision* access is available to the on-site IR authority, open a *RiskVision* ticket to document the occurrence of an incident.	RiskVision *is the HHS enterprise tool that provides for Departmental incident tracking and reporting. Coordinate with the CSIRT to ensure duplicate tickets are not created.*
4. Coordinate with the CSIRT to perform the following applicable actions:	*Several of these procedures may be required– some may need to be performed in parallel.*
a. For *Worm Infections*, perform the actions in Section 2.1.7.	
b. For *Windows Intrusions*, perform the actions in Section 2.1.8.	
c. For *Unix Intrusions*, perform the actions in Section 2.1.9.	
d. For *Denial of Service (DoS)*, perform the actions in Section 2.1.10.	
e. For *Malicious Network Behavior*, perform the actions in Section 2.1.11.	
f. For *Website Defacement*, perform the actions in Section 2.1.12.	
g. For *Blackmail*, perform the actions in Section 2.1.13.	
h. For *Smartphone Malware*, perform the actions in Section 2.1.14.	

PROCEDURE	PRINCIPLE
i. For *Social Engineering*, perform the actions in Section 2.1.15.	
j. For *Information Leakage*, perform the actions in Section 2.1.16.	
k. For *Insider Abuse*, perform the actions in Section 2.1.17.	
l. For *Phishing*, perform the actions in Section 2.1.18.	
m. For all others, coordinate directly with, and under the direction of, the CMS CSIRT to perform the applicable actions.	
5. Verify that all of the specific steps of the procedures referenced in Step 4 above have been completed **BEFORE proceeding to the next step.**	
2.1.3 CMS CSIRT RESPONSE	*Upon notification of an incident, the CMS CSIRT performs these actions.*
2.1.3.1 PROCEDURE USERS	
1. CMS CSIRT personnel.	
2.1.3.2 ENTRY CONDITIONS	
1. A *Security/Privacy Incident, Reportable Event*, or data *Breach* is believed, or suspected, to have occurred.	
2. The *Incident, Reportable Event*, or *Data Breach* has been reported to the on-site IR authority.	
3. The *Incident, Reportable Event*, or *Data Breach* has been reported to CMS.	
4. The *Incident, Reportable Event*, or *Data Breach* has been reported to the CMS CSIRT by the *CMS Service Desk*, or any *other* entities.	

PROCEDURE	PRINCIPLE
2.1.3.3 CMS CSIRT RESPONSE PROCEDURE	
1. Establish communications with:	*This does **not** mandate a continuous uninterrupted communications link. The CSIRT need only ensure consistent and reliable POCs, with reliable methods, are identified and instituted.*
a. The *on-site IR authority.*	*To coordinate further response actions.*
b. The CMS SOC, as applicable.	*To gather additional traffic and perimeter defense information and coordinate response actions.*
c. The POC for the CMS *Business Owner(s)* for the affected system(s).	*To coordinate actions that may affect operations for the applicable system(s).*
2. Re-assess the *Incident Category* in accordance with Figure 1.	*To verify and update the initial incident categorization. This process may need to be performed again several times, as facts and conditions are updated.*
3. If not already created, open a *RiskVision* ticket to document the occurrence of an incident.	RiskVision *is the HHS enterprise tool that provides for Departmental incident tracking and reporting.*
NOTE: **Privacy incidents must be reported to the HHS CSIRC within *one hour* of discovery.**	*In accordance with OMB Memorandum M-07-16,* Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
4. Report/coordinate to the HHS CSIRC.	*It is the responsibility and authority of the* HHS Computer Security Incident Response Center *(CSIRC) to further report to the* United States Computer Emergency Readiness Team *(US-CERT).*

PROCEDURE	PRINCIPLE
5. If PII is involved, the CMS CSIRT commences the *CSIRT Privacy Incident Analysis* of Section 2.1.4:	*PII also includes PHI and FTI.*
a. While *concurrently* completing this procedure, proceed to Section 2.1.4, *CSIRT Privacy Incident Analysis,* for further ***additional*** actions.	*If a privacy incident involving of PII, perform the remaining steps of this procedure while* ***concurrently*** *performing the* CSIRT Privacy Incident Analysis *of Section 2.1.4.*
b. Continue with this procedure in coordination with, and in parallel to, the *CSIRT Privacy Incident Analysis* of Section 2.1.4.	
6. If *Classified Material* is suspected of being involved:	
a. Contact CMS *Physical Security* Office.	*The CMS SOC maintains the appropriate CMS OOM/ASG/DCIP (Division of Critical Infrastructure Protection) POC information in the CMS SOC* Incident Handling *standard operation procedure*.
b. Continue with this procedure in coordination with the CMS physical security authority.	
7. If criminal activity is suspected:	
a. Report the incident to the *Office of the Inspector General (OIG), Special Investigation Unit (SIU).*	*Report to oiccu@oig.hhs.gov.*
b. Continue with this procedure in coordination with the OIG SIU.	
8. Coordinate with the on-site IR authority to perform the following applicable actions:	*Several of these procedures may be required– some may need to be performed in parallel.*
a. For *Worm Infections*, perform the actions in Section 2.1.7.	
b. For *Windows Intrusions*, perform the actions in Section 2.1.8.	
c. For *Unix Intrusions*, perform the actions in Section 2.1.9.	

PROCEDURE **PRINCIPLE**

d. For *Denial of Service (DoS)*, perform the actions in Section 2.1.10.

e. For *Malicious Network Behavior*, perform the actions in Section 2.1.11.

f. For *Website Defacement*, perform the actions in Section 2.1.12.

g. For *Blackmail*, perform the actions in Section 2.1.13.

h. For *Smartphone Malware*, perform the actions in Section 2.1.14.

i. For *Social Engineering*, perform the actions in Section 2.1.15.

j. For *Information Leakage*, perform the actions in Section 2.1.16.

k. For *Insider Abuse*, perform the actions in Section 2.1.17.

l. For *Phishing*, perform the actions in Section 2.1.18.

m. For all others, coordinate directly with, and under the direction of, the IR authority, the CMS CISO, and the HHS CSIRC, as applicable, to perform the response actions.

9. If a forensic response is required, coordinate the forensic response as follows:

a. Identify possible sources of forensic data. Coordinate with the HHS CSIRC as required.

b. Acquire the forensic data. Coordinate with the HHS CSIRC as required.

(1) Develop a plan to acquire forensic data.

PROCEDURE	PRINCIPLE
(2) Coordinate with the on-site IR authority to acquire the forensic data.	
(a) Secure/confiscate applicable equipment.	
(b) Secure/confiscate applicable software.	
(c) Secure/confiscate applicable system logs.	
(3) Coordinate with the HHS CSIRC and the on-site IR authority to verify the integrity of the forensic data.	
10. Verify that all of the specific steps of the procedures referenced in Step 8 above have been completed *BEFORE proceeding to the next step*.	
11. After management approval has been acquired to *recover* from the incident, proceed to the following steps:	*Management approval may include on-site management, CMS CSIRT, CMS, CSIRC, and/ or the US-CERT, as appropriate.*
NOTE: **Carefully monitor all applicable resources after EACH of the following steps BEFORE proceeding to the next step.**	*Monitor the applicable resources to determine if the malware has been removed effectively. If ANY indications of infection re-emerge, stop the process and combat the attack before proceeding to the next step.*
a. Reopen the network traffic that was used as a propagation method by the attack.	
b. Reconnect the affected sub-areas together.	
c. Reconnect the mobile devices to the affected area.	
d. Reconnect the affected area to the local network.	
e. Reconnect the affected area to the Internet.	
12. Collaborate with appropriate legal teams if a legal action is in process.	

PROCEDURE	PRINCIPLE
13. In case of new vulnerability discovery (*zero-day-exploit*):	*CSIRT coordinate through CSIRC and US-CERT.*
a. Report to the applicable vendor.	
b. Follow-up with the vendor to receive applicable patches and fixes as soon as they become available.	
14. Collect *lessons-learned*:	*This should occur no less than 7 days after recovery from the incident.*
a. Consider what preparation steps could have taken to respond to the incident faster or more effectively.	
b. If necessary, adjust assumptions that affected the decisions made during incident preparation.	
c. Assess the effectiveness of the organization's response process, involving people and communications.	
d. Consider what relationships inside and outside of organizations could help with future incidents.	
15. Debrief and closeout incident as follows:	
a. Measure response effectiveness.	*Perhaps the organization responded too quickly, or the organization needs to improve response time and add new steps.*
b. If required, prepare and add new information to the CSIRT incident standard operating procedures.	*This should be provided for in the basic standard operating procedure, and someone on the team should have the authority to makes specific changes.*
c. Prepare a final report per Section 2.1.19.	
d. Distribute the final written report to:	*Include an honest evaluation of the team's response, damage estimates, and any major recommendations for procedural changes.*
(1) CMS CISO.	
(2) Applicable Business Owner.	

PROCEDURE	PRINCIPLE
(3) On-site incident response authority. (4) HHS CSIRC, via RiskVision. 16. Close *RiskVision* Ticket.	

2.1.4 CSIRT PRIVACY INCIDENT ANALYSIS

2.1.4.1 PROCEDURE USERS

1. CMS CSIRT personnel.

2.1.4.2 ENTRY CONDITIONS

1. A *Privacy Incident* is believed, or suspected, to have occurred.

2. A *Privacy Incident* has been reported to CMS.

3. The *Privacy Incident* has been reported to the CMS CSIRT by the *CMS Service Desk*, or any *other* entities.

2.1.4.3 CSIRT PRIVACY INCIDENT ANALYSIS PROCEDURE

1. Document the results of this procedure in the *Assessment for Risk of Harm to Individuals for PII/PHI Data Breach* Excel worksheet. Maintain this worksheet with the applicable *Incident Report* generated in Section 2.1.19, *Preparing the Computer Security Incident Report (CSIR).*	*The* Assessment for Risk of Harm to Individuals for PII/PHI Data Breach *Excel worksheet is available at* *http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.*

PROCEDURE	PRINCIPLE
2. Refer to the *Breach Assessment Guidelines* of Table 1 and the *Breach Assessment and Notification Process* of Figure 2 while performing the following:	
a. If hard copy documents containing PII/ PHI have gone to the wrong ***provider***, perform the following:	*For example: CMS business associate (e.g., MAC, FI, Carrier, other Medicare contractor) sends remittance advice to wrong provider. Data elements may include full HICN, beneficiary name, address, DOB, procedure codes, claims info. (See Table 1.)*
(1) CSIRT documents that the incident falls within the *Breach Assessment Guidelines* of Table 1.	
(2) CSIRT coordinates operational mitigation activities/corrective action with business associate as appropriate.	*This may include outreach and education.*
(3) CSIRT instructs applicable *providers* to destroy PII/PHI and alert applicable contractors to mismailing.	*Providers are obligated to protect the privacy and security of PII/PHI received in the same or similar manner as the CMS business associate that disclosed the information.*
(4) CSIRT adds the incident to the monthly CSIRT report to HHS CSIRC.	
(5) Resume coordination with the CSIRT response. Do NOT refer to the *Pre Breach Analysis Team* (Pre-BAT).	

PROCEDURE	PRINCIPLE
b. If hard copy documents containing PII/ PHI, go to wrong ***beneficiary.***	*For example: CMS business associate (e.g., MAC, FI, Carrier, other Medicare contractor) sends Medicare Summary Notice to wrong beneficiary. Data elements may include last 4 digits of HIC number, beneficiary name, address, DOB, procedure codes, claims info. (See Table 1).*
(1) CSIRT documents that the incident falls within the *Breach Assessment Guidelines* of Table 1.	*Low likelihood of significant financial, reputational, or other harm to affected beneficiary. 1) beneficiary reported mismailing to business associate, PII/PHI not intentionally accessed; very little likelihood beneficiary knew the other; 2) low risk of financial harm resulting in ID theft given data elements contained in MSN (not complete SSN/HICN); 3) Procedure code may be included but not diagnostic info.*
(2) CSIRT coordinates operational mitigation activities/corrective action with business associate as appropriate.	*This may include outreach and education.*
(3) CSIRT adds the incident to the monthly CSIRT report to HHS CSIRC.	
(4) Resume coordination with the CSIRT response. Do ***NOT*** refer to the *Pre Breach Analysis Team* (Pre-BAT).	
3. If the privacy incident meets any of the *Breach Assessment Guidelines* of Table 1:	
a. Document such in the *Incident Report*, exit this procedure, and return to the security incident handling procedure.	

PROCEDURE	PRINCIPLE
4. If the privacy incident does ***not*** meet any of the guidelines in the *Breach Assessment Guidelines* of Table 1, determine if the privacy incident involves *secured* PII that has been rendered *unusable*, *unreadable*, or *indecipherable* in accordance with the HHS guidance.	*"Secured" means that it was encrypted in accordance with FIPS 140-2. HHS guidance is provided at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.*
a. If the PII has been determined to be *unsecured*:	
(1) The *Incident Response Lead* (IR Lead) must refer the potential PII breach to the *Pre-Breach Analysis Team* (Pre-BAT.).	*The Pre-BAT reviews and triages PII-related incidents, and forwards to the full Breach Analysis Team (BAT) for a formal risk assessment.*
(2) *IR Lead* proceeds, with the *Assessment for Risk of Harm to Individuals for PII/PHI Data Breach* Excel worksheet, to *Pre-Breach Analysis Team Actions* in Section 2.1.5.	*The worksheet shall be updated and completed by the Pre-BAT, and if necessary, the BAT.*
b. If the PII is *secured*:	*"Secured" means that it was encrypted in accordance with FIPS 140-2. HHS guidance is provided at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.*
(1) Exit this procedure and continue with *CMS CSIRT Response*, actions in Section 2.1.3.	

2.1.5 PRE-BREACH ANALYSIS TEAM ACTIONS

2.1.5.1 PROCEDURE USERS

1. CMS Pre-BAT assigned personnel.	*Pre-BAT consist of the following personnel (or designates): CMS CISO, applicable CMS Business Owner, the CMS Privacy Officer, and the CMS Senior Official for Privacy.*

PROCEDURE	PRINCIPLE
2.1.5.2 ENTRY CONDITIONS	
1. A *Privacy Incident* is believed, or suspected, to have occurred.	
2. A *Privacy Incident* has been reported to CMS.	
3. The *Privacy Incident* has been reported to the CMS CSIRT by the *CMS Service Desk*, or any *other* entities.	
4. The CSIRT team has referred a *privacy incident* to the Pre-BAT for further disposition.	
2.1.5.3 PRE-BAT TEAM PROCEDURES	
1. Pre-BAT, continues to update the *Assessment for Risk of Harm to Individuals for PII/PHI Data Breach* Excel worksheet with applicable information throughout this procedure.	*The worksheet shall be updated and completed by the Pre-BAT, and if necessary, forwarded to the BAT.*
2. If the privacy incident meets any of the *Breach Assessment Guidelines* of Table 1:	*While this step was conducted by the CSIRT already, additional information may have become available that may change the outcome of this analysis.*
a. Refer back to the CSIRT to coordinate operational mitigation activities/corrective action with business associate as appropriate.	
b. Exit this procedure and return to the security incident handling procedure.	

PROCEDURE	PRINCIPLE
3. Determine if the privacy incident involves *secured* PII that has been rendered *unusable*, *unreadable*, or *indecipherable* in accordance with the HHS guidance.	
a. If the PII is *secured*:	*"Secured" means that it was encrypted in accordance with FIPS 140-2. HHS guidance is provided at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.*
(1) Refer back to the CSIRT to coordinate operational mitigation activities/ corrective action with business associate as appropriate.	
(2) Exit this procedure and return to the security incident handling procedure.	
4. Determine if a *breach* of PII ***may*** have occurred. A breach ***may*** have occurred if *any* of the following events has occurred:	*A privacy incident **may** not rise to the level of a "Breach" until it has been determined that the use or disclosure of the protected information compromises the security or privacy of the protected individual and poses a reasonable risk of harm to the applicable individuals.* ***The Breach Risk Assessment is performed by the full BAT.*** *The goal if this step is to determine if the **possibility** of a breach exists.*
a. A CMS organization has *lost control* of PII in a usable form (either physical or electronic), such that it has left the organizational boundaries of CMS (or its contractors.)	
b. A CMS organization has allowed an *unauthorized disclosure* of PII, in a usable form (either physical or electronic), to *any* organization to which it is not authorized to disclose.	*Note that this includes unauthorized disclosures or inspections of* Federal Tax Information (FTI) *as defined in the IRS Publication 1075,* Tax Information Security Guidelines for Federal, State and Local Agencies *(available at http://www.irs.gov/pub/irs-pdf/p1075.pdf.)*

PROCEDURE	PRINCIPLE
c. An *unauthorized individual or entity* has *accessed* PII, in a usable form (either physical or electronic), while in the custody of a CMS organization.	
d. An *authorized individual or entity* has *accessed* PII, in a usable form (either physical or electronic), for an *unauthorized* purpose.	
5. If a breach ***has not*** occurred (as defined in Step 4 above):	
a. Coordinate with the CSIRT to update and close the applicable *RiskVision* ticket.	
b. Return to the calling procedure and perform any remaining steps.	
6. If a breach ***may*** have occurred (as defined in Step 4 above), perform the following:	
a. Coordinate and convene the full *Breach Analysis Team* (BAT) to conduct a formal risk assessment of the privacy incident.	
b. Collect the following information necessary to conduct a *Breach Risk Assessment*:	*This is ONLY a* collection *process. Evaluation and assessment will be made by the full BAT.*
(1) Description of what happened.	*Be sure to collect all of the pertinent events, the timeline, and the individuals involved.*
(2) Type of PII/PHI involved.	*Type: Social Security numbers (SSNs), photographic identifiers, financial account information, phone numbers, etc. Be specific and identify* **all** *the fields involved (not just the ones that "contain PII/PHI".*
(3) To whom does the PII/PHI pertain?	*To whom the PII/PHI refers: Employees, patients, etc.*
(4) Description of controls in place that could potentially minimize the risk posed by the incident.	*e.g., "Was the information encrypted, even in a non-FIPS compliant fashion"; "Was the exposure only limited to employees and contractors, or other covered entities?"*

PROCEDURE	PRINCIPLE
(5) Remediation actions taken to minimize the risk of the incident.	*"What steps have already been taken?" "What steps are in the process of being taken?"*
(6) Approximate number of potentially impacted individuals affected by the incident.	*The magnitude of the number of affected individuals may dictate the method(s) CMS chooses for providing notification, but will* ***not*** *be the determining factor for whether CMS will provide notification.*
(7) Preliminary *Breach Risk Assessment* risk assessment results.	*OPDIVs can conduct a risk assessment on incidents in addition to the risk assessment conducted by the HHS PIRT. OPDIVs that conduct a risk assessment should communicate the initial results of their risk assessment to the HHS PIRT for review and validation.*
c. If the potential breach may include FTI:	*FTI is Federal Tax Information as defined in IRS Publication 1075.*
(1) CSIRT IR Lead coordinates with the CMS CISO to:	
(a) Contact the office of the appropriate Special Agent-in-Charge, *Treasury Inspector General for Tax Administration (TIGTA).*	*TIGTA Field Agent contact information (for applicable Field Divisions) is located in the IRS Publication 1075.* *TIGTA Hotline Number is: 1-800-589-3718.* *TIGTA Web Site: www.treas.gov/tigta.*
(b) Prepare and send a *Data Incident Report* to the *IRS Office of Safeguards* that includes the following:	
i. Name of agency (CMS) and CMS point of contact for resolving data incident with their contact information.	
ii. Date and time of the incident.	
iii. Date and time the incident was discovered.	
iv. How the incident was discovered.	

PROCEDURE	PRINCIPLE
v. Description of the incident and the data involved.	*Include specific data elements if known.*
vi. Potential number of FTI records involved.	*If unknown, provide a range if possible.*
vii. Specific address/location where the incident occurred.	
viii. Information technology involved.	*Example: laptop, server, mainframe.*
CAUTION: **Do not include *ANY* FTI in the email message or the attached *Data Incident Report* sent to the *IRS Office of Safeguards*.**	
ix. Email the *Data Incident Report* to the SafeguardReports@IRS.gov mailbox.	*Reports should be sent electronically and encrypted via IRS approved encryption techniques. Use the term "Data Incident Report" in the subject line of the email.*
d. IR Lead and Pre-BAT lead proceed, with the *Assessment for Risk of Harm to Individuals for PII/PHI Data Breach* Excel worksheet, to Section 2.1.6, *Breach Analysis Team Actions*.	*The worksheet shall be updated by the Pre-BAT and forwarded to the BAT to be included as an attachment to the* CMS Computer Security Incident Report (CSIR).

2.1.6 BREACH ANALYSIS TEAM ACTIONS

2.1.6.1 PROCEDURE USERS

1. CMS BAT assigned personnel.

2.1.6.2 ENTRY CONDITIONS

1. A *Privacy Incident* is believed, or suspected, to have occurred.

PROCEDURE	PRINCIPLE
2. A *Privacy Incident* has been reported to CMS.	
3. The *Privacy Incident* has been reported to the CMS CSIRT by the *CMS Service Desk*, or any *other* entities.	
4. A *Privacy Incident* has been referred to the CMS BAT by the CMS Pre-BAT.	

2.1.6.3 BREACH ANALYSIS TEAM PROCEDURE

1. Conduct a *Risk Assessment*, and document in the *Assessment for Risk of Harm to Individuals for PII/PHI Data Breach* Excel worksheet, to determine the risk of harm to the affected individuals. Consider the following elements:	*To determine the risk to individuals whose PII/PHI has been compromised, the risk of harm, and the extent of notification required.*
a. The nature of the data elements breached.	*In assessing the levels of risk and harm, CMS and HHS management will consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.*
b. The number of individuals affected.	
c. The likelihood that the information is *accessible* and *usable.*	*The likelihood the information will be recognized, accessed, and used by unauthorized individuals, will influence the decision to notify.*
d. The likelihood that the breach may lead to *harm.*	*There are two factors that should be addressed; 1) The broad reach of potential harm, and 2) The likelihood harm will occur.*
e. Ability of CMS to mitigate the risk of harm.	*Within an information system, the risk of harm will depend on how CMS is able to mitigate further compromise of the system(s) affected by a breach.*

PROCEDURE	PRINCIPLE
2. Document the results of the above risk assessment on the *Assessment for Risk of Harm to Individuals for PII/PHI Data Breach* Excel worksheet, and submit the completed form to the CMS *Senior Official for Privacy*.	*The* Assessment for Risk of Harm to Individuals for PII/PHI Data Breach *Excel worksheet is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html*.
3. If the above risk assessment indicates that the *risk of financial, reputational, or other harm to the individual* is ***NOT*** *significant*, coordinate with the CSIRT to update and close the applicable *RiskVision* ticket.	
4. If the above risk assessment indicates that the *risk of financial, reputational, or other harm to the individual* is *significant*, coordinate with the HHS PIRT to perform the following:	
a. The CMS Senior Official for Privacy and Business Owner coordinate to notify, without unreasonable delay, the individuals affected.	*In accordance with OMB Memorandum M-07-16,* Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
b. If the information involved in the breach contains PHI:	*This step does not apply unless* PHI *(as defined by HIPAA) is involved. If the data is only* PII *(as defined by the Privacy Act), then proceed to Step 5.*
(1) If the PHI breach involves more than 500 individuals:	
(a) The CMS Senior Official for Privacy and Business Owner coordinate to notify HHS OCR of the breach via the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.	*Provide the Secretary with notice of the breach without unreasonable delay and in no case later than 60 days from discovery of the breach.*
(2) If the PHI breach involves more than 500 residents of a State or Jurisdiction:	
(a) The CMS Senior Official for Privacy and Business Owner coordinate to notify prominent media outlets serving the applicable State or Jurisdiction of the breach.	

PROCEDURE	PRINCIPLE
5. Verify all of the above steps have been completed fully and satisfactorily.	
6. Coordinate with the CSIRT to update and close the applicable *RiskVision* ticket.	

2.1.7 WORM INFECTION

2.1.7.1 PREPARATION

1. Define participants.	*Who will be involved in combating this threat? These individuals should be documented in a contact list, and kept permanently up to date.*
2. Ensure availability of tools.	*Make sure that analysis tools are available (antivirus, IDS, logs analyzers), not compromised, and up to date.*
3. Maintain accurate documentation of the network topology.	*Make sure to have architecture map of applicable networks.*
4. Maintain accurate documentation of the applicable assets.	*Make sure that an up-to-date inventory of the assets is always available. The SSP or network scanning processes should assist.*
5. Maintain a continuous monitoring of the environment, and maintain awareness.	*Perform a continuous security watch and inform the appropriate people about current threat trends.*

2.1.7.2 IDENTIFICATION

1. Analyze input from the following sources:	*This should be part of the continuous monitoring process.*
a. Antivirus logs.	
b. Intrusion Detection Systems (IDS).	
c. Suspicious connection attempts on servers.	
d. High occurrence of account locking.	

PROCEDURE	PRINCIPLE
e. Suspicious network traffic.	
f. Suspicious connection attempts in firewalls.	
g. High increase in support calls.	
h. High system loads or system freezes.	
i. High volumes of email.	
2. Identify the threat by coordinating and utilizing the following resources:	*These resources may also be monitoring the applicable infrastructure and may have noticed other applicable trends.*
a. Coordinate with the CMS CSIRT.	
b. Coordinate with the HHS CSIRC.	
c. Coordinate with the US-CERT.	
d. Coordinate with other CMS contractor CERT teams.	*Other CMS organizations may be under attack. A coordinated response may prove to be much more effective.*
e. Reference CERT bulletins.	
f. Coordinate with external support contacts (antivirus companies, etc.)	
g. Reference external websites for emerging threats.	*Secunia, SecurityFocus, etc., may provide up-to-date information on emerging or developing attacks.*
h. Coordinate with affected Business Owners and senior management.	*Business Owners may have insight on why specific resources or processes are being targeted.*
3. Assess and define the boundaries of the infection (i.e., global infection, bounded to a subnet, or subsystem, etc.).	*If possible, identify the business impact of the infection.*

PROCEDURE	PRINCIPLE
2.1.7.3 CONTAINMENT	*Objective: Mitigate the attack's effects on the targeted environment.*
1. Disconnect the infected area from the internet.	*Some worms rely on external servers to download additional malware. Disconnecting reduces the opportunity for spread, and limits access to potential "command-and-control" resources.*
2. Isolate the infected area of the infrastructure.	*Disconnect it from any other networks or subnets, as appropriate.*
a. If business-critical traffic cannot be disconnected, allow it only after ensuring that it cannot be an infection vector or find validated circumventions techniques.	*If possible, severely restrict the routing of traffic to-and-from the infected resources to only those **absolutely** necessary to perform the business-critical processes.*
3. Neutralize the propagation vectors.	*A propagation vector can be anything from network traffic to software flaw.*
4. Apply relevant countermeasures.	*Patch, traffic blocking, disable devices, etc. For example, the following techniques can be used: Patch deployment tools (WSUS), Windows GPO, Firewall rules, and/or Operational procedures.*
5. Repeat steps 2 to 4 on each sub-area of the infected area until the worm stops spreading.	*If possible, continually monitor the infection using analysis tools (antivirus consoles, server logs, support calls, etc.).*
6. Block and/or monitor mobile devices, as appropriate.	*Make sure that no laptop, PDA, or mobile storage can be used as a propagation vector by the worm.*
7. Inform and direct end-users, as appropriate.	*Inform end-users of the event and ensure users follow directives precisely. Make them part of the solution as opposed to an "irritant" in the recovery process.*

PROCEDURE	PRINCIPLE
2.1.7.4 REMEDIATION	*Objective: Take actions to stop the malicious worm behavior.*
WARNING: **Some worms can block some of the remediation deployment methods.**	*If this occurs, workarounds will be required.*
1. Identify tools and remediation methods.	*The following resources should be considered: Vendor fixes (Microsoft, Oracle, etc.), antivirus signature database, External support contacts, and/or Security websites.*
2. Coordinate with the managing authority to define a disinfection process.	*The process should be validated by higher authority, such as the CSIRT, CSIRC and/or the US-CERT, as appropriate.*
3. Test the proposed remediation method.	*Test the disinfection process and make sure that it properly works without damaging any essential services.*
4. Deploy the remediation method.	*Deploy the disinfection tools. Several options can be used, including: Windows WSUS, GPO, antivirus signature deployment, Manual disinfection, and/or other available tools.*
5. Monitor progress.	*Remediation progress should be monitored by the on-site IR authority, in coordination with the CMS CSIRT, and the CMS SOC as applicable.*
2.1.7.5 RECOVERY	*Objective: Restore the system to normal operations.*
1. Verify all previous steps have been completed correctly.	
2. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*

PROCEDURE	PRINCIPLE
2.1.8 WINDOWS INTRUSION	Intrusion *includes detection of* Malware *on a Windows-based system.*
2.1.8.1 PREPARATION	*Objective: Establish contacts, define procedures, and gather information to save time during an attack.*
1. Develop processes and procedures for providing *physical* access to suspicious systems to applicable forensic investigators.	*Physical access is preferred to remote access, since the hacker could detect the investigations done on the system (by using a network sniffer for example). If necessary, physical access may be required to disconnect the suspected machine from any network.*
2. Develop a process for creating copies of affected hard disks for forensic and evidence support.	
3. Establish baseline knowledge of *normal* network activity of assets within the applicable infrastructure.	*Organizations should maintain records describing the usual port activity to compare to the current (abnormal?) state.*
4. Establish baseline knowledge of the *normal* services running on assets within the applicable infrastructure.	*Baseline configuration standards become extremely helpful here. In addition, applicable System Security Plans should accurately show deviations from approved baselines.* *The more information that is available on an asset's "clean state", the higher the success rate in detecting fraudulent activity.* *One method is to establish and maintain a regularly updated list, including cryptographic hash values (MD5s) of all critical files, stored in a secure place, off of the network, or even on paper. Another is to establish and maintain a map of usual port and Unix socket activity/traffic rules. Another method is to establish and maintain a whitelist of known good system "hooks".*

PROCEDURE	PRINCIPLE
2.1.8.2 IDENTIFICATION	*Note that Microsoft* Sysinternals *Troubleshooting Utilities can be used to perform many applicable tasks.*[1]
CAUTION: **A Rootkit may change the results for many of the command-line steps in this procedure. Administrators should be aware that the readings they are observing might not be indicative of *actual* conditions.**	
1. Antivirus symptoms:	
a. Antivirus raising an alert.	
b. Unable to update its signature.	
c. Failing to run, is disabled, or unable to run (even manually).	
2. Hard-disk symptoms.	*Hard drive is conducting large or unusual operations at unexpected times.*
3. Unusually slow computer.	*While a computer has usually been delivering "good performance", it suddenly or recently "got slower."*
4. Network activity symptoms.	*Internet or network connection is slow.*
5. Other symptoms:	
a. Computer reboots without reason.	
b. Applications are crashing.	
c. Pop-up windows are appearing while browsing on the web.	*Sometimes even without browsing.*
d. IP address (if static) is *blacklisted* on one or more Internet *Black Lists.*	
e. People are complaining about an organizational user sending email or instant message.	

[1] More information about *Sysinternals* is available from Microsoft at http://technet.microsoft.com/en-us/sysinternals.

PROCEDURE	PRINCIPLE
f. Unusual accounts created, especially in the *Administrators* group.	*Useful commands may include:* *C:\> lusrmgr.msc* *or* *C:\> net localgroup administrators.*
g. Unusually large files on the storage support.	*Bigger than 10 MB (for instance) may be an indication of a system compromised for illegal content storage. Look for unusual files added recently in system folders, especially C:\WINDOWS\system32.* *Look for files using the "hidden" attribute:* *C:\> dir /S /A:H* *(Other utilities may be available to conduct more systematic analysis, such as "windirstat".)*
h. Unusual programs launched at boot time in the Windows registry, especially:	*Especially check in:* *- HKLM\Software\Microsoft\Windows\ CurrentVersion\Run.* *- HKLM\Software\Microsoft\Windows\ CurrentVersion\Runonce.* *- HKLM\Software\Microsoft\Windows\ CurrentVersion\RunonceEx.* *Useful tools may include* HiJackThis.
(1) Look for unusual programs launched at boot time in the user's *Startup* folder.	*Look in: C:\Documents and Settings\USER\ Start Menu\Programs\Startup, or their version-specific equivalent (e.g., C:\WinNT\ Profiles\user\Start Menu\Programs\Startup.)*
i. Discrepancies in hardware/software clocks.	
6. Check all running processes for unusual or unknown entries.	*Especially check processes with username "SYSTEM" and "ADMINISTRATOR". Tools include:* *C:\> taskmgr.exe (or tlisk, tasklist depending on Windows release), or the* Sysinternals *tool* "Process Explorer".
7. Look for unusual/unexpected network services installed and started.	*Use: C:\> services.msc, or* *C:\> net start, or their equivalent.*

PROCEDURE	PRINCIPLE
8. Look for unusual network activity:	
a. Check for file shares and verify each one is linked to a normal activity.	*Use: C:\> net view \\127.0.0.1 or the* Sysinternals *tool* "TCPView".
b. Look at the opened sessions on the machine.	*C:\> net session.*
c. Look at the sessions the machine has opened with other systems.	*C:\> net use.*
d. Check for any suspicious NETBIOS connections.	*C:\> nbtstat –S.*
e. Look for any suspicious activity on the system's ports.	*C:\> netstat –na 5 (the "5" refreshes each 5 seconds.)* *Use –o flag for Windows XP/2003 to see the owner of each process:* *C:\> netstat –nao 5.*
f. Use a sniffer (*Wireshark, tcpdump* etc.) and see if there are unusual attempts of connections to or from remote systems.	*If no suspicious activity is witnessed, try using the sniffer while browsing some sensitive websites (banking website for example) and see if there is any particular network activity.*
9. Look at the list of scheduled tasks for any unusual entry.	*C:\> at* *On Windows 2003/XP* *C:\> schtasks.*
10. Look at log files for unusual entries.	*C:\> eventvwr.msc. Look for events like: "Event log service was stopped", "Windows File Protection is not active", "The protected System file <name> was not restored to its original", "Telnet Service has started successfully", or other unusual activity.*
11. Search for events affecting the firewall, the antivirus, the file protection, or any suspicious new service:	
a. Look large amounts of failed login attempts or locked out accounts.	
b. Watch firewall log files for suspicious activity.	

PROCEDURE	PRINCIPLE
12. Look for *rootkits.*	*Run the* Sysinternals *tool* "Rootkit Revealer*" and/or other comparable tools such as; "*Rootkit Hooker*", "*Ice Sword*", "*Rk Detector*", "*SysInspector*", "*Rootkit Buster*", or other professional level tools.* *It is better to run several of these tools to ensure better coverage of known rootkits.*
13. Run *at least* one antivirus product on the whole disk.	*If possible, use* several *antivirus tools. The antivirus must* absolutely *be up-to-date.*

2.1.8.3 CONTAINMENT

1. Coordinate with the on-site IR authority to perform the following:	
a. Contain the damage as follows:	
(1) Logically isolate any affected device(s) from the network by blocking the applicable IP(s) at security routers or firewalls, both inbound and outbound.	
(2) If the *CSIRT Lead* (in coordination with the OIG SIU) determines that computer *forensic* support is required:	*Forensic support is "required" when the collection (or preservation) of evidence for possible use in a criminal or civil prosecution is desired.*
(a) Immediately establish communications with the on-site forensic support team and coordinate future actions through the CMS SOC.	*This does **not** mandate a continuous uninterrupted communications link. The CSIRT need only ensure consistent and reliable POCs, with reliable methods, are identified and instituted.*
(b) Instruct the on-site forensic support team to secure the physical scene of any affected asset(s).	*Do not allow **anyone** other than the* on-site IR authority *access to the scene.*
(c) Unless directed by the CMS SOC:	
i. ***DO NOT** power-down* any applicable device(s).	

PROCEDURE	PRINCIPLE
ii. ***DO NOT*** allow the asset(s) user/owner access to the device(s).	
iii. ***DO NOT*** run ***any*** programs or utilities on the affected device(s).	
iv. ***DO NOT*** view or access ***any*** files on the affected device(s).	
(3) If instructed by the HHS CSIRC, power-down affected machines.	*Include contingency plans for this step, as some infections will cause **additional damage** if the host is disconnected from the network. For example, some infections may ping another server, and if those ping attempts fail, the infection may proceed to overwrite hard drive data.*
(4) Secure backups.	*Do not risk compromising backups before the system is completely purged of infection.*
(5) Secure system logs.	*This is essential so investigators can later identify any damage.*
(6) Record incident details.	*Record the time, machine ID, symptoms, and any/all actions taken.*
b. Remove infection as follows:	
(1) Disable and delete malicious code.	*Where possible, use specialized commercial tools. Antivirus vendors may recommend that a special tool be used because normal malware removal procedures may not be completely effective on some blended threats.*
(2) Install and run antivirus software with the latest signature file.	*Do this after using any removal tool and be sure the latest data cover the threat just removed.*
(3) Install and run dedicated anti-spyware software with the latest signature file.	*Run a complete anti-spyware scan, separate from the full antivirus scan. Remove all found infections.*

PROCEDURE	PRINCIPLE
c. Evaluate the damage as follows:	
(1) Locate the source of infection.	*Find how the malware entered the system—this will aid in locating damage as well as preventing future incidents. Insider attacks/ platforms are common and the most dangerous.*
(2) Coordinate with the antivirus vendor and the HHS CSIRC to determine the payload.	
(3) Check to see if the payload was actually activated.	*Do this by verifying the integrity of code or data that would be attacked by the payload.*
2. If the machine is considered mission essential and cannot be disconnected, perform the following:	*Most machines are NOT mission-essential. Any that are, should be identified clearly in the SSP and the CP, and appropriate actions should already be pre-identified for this specific scenario.*
a. Reboot from a live CD.	
b. Backup all-important data in case the hacker notices the ongoing investigation and starts deleting files.	*Also, make a copy of the system's memory for further analysis. (Use tools such as Memoryze, win32dd, etc.)*
c. Boot into a CD containing disinfection tools or a dedicated antivirus live CD.	*They can usually be found on the applicable antivirus company's websites.*
d. Complete any other cleaning required to clean the system.	
e. Run a full antivirus scan.	
f. Cold-reboot the machine.	Cold-reboot *means secure all power for at least 30-seconds.*
g. Perform *another* full virus scan of the system, hard disks, and memory.	

PROCEDURE	PRINCIPLE
3. If the machine is not considered mission-essential, perform the following:	*Pull the network plug off physically, to prevent more infection on the network and to stop possible illegal action being done from the affected computer (the malware could send spam massively, take part in a DoS attack, or store illegal files on the system for example).*
a. Shut the machine down by removing its power plug.	*If it is a laptop with a battery on, just push the "off" button for some seconds until the computer switches off.*
b. Reinstall the OS and applications and restore user's data from a trusted backup.	
4. Start offline investigations immediately if the live analysis did not give any result.	*The system should still be considered compromised until proven otherwise.*
5. Make a copy (bit by bit) of the whole hard disk on an external storage media.	*Use tools such as EnCase, X-Ways, or similar forensic tools (dd, ddrescue etc.).*
6. Try to find evidences of every action of the hacker:	
a. Find all files used by the attacker.	*This should include* deleted files *(use forensic tools) to see what has been done with them or their functionality, in order to evaluate the threat.*
b. Check all files accessed recently.	
c. Inspect network shares to see if the malware has spread through it.	
d. Determine how the attacker gained access to the system.	*All leads should be considered. If no computer proof of the intrusion is found, never forget it could come from a physical access or a complicity/stealing of information from an employee/contractor.*
7. Identify and isolate the suspect binaries.	

PROCEDURE	PRINCIPLE
2.1.8.4 REMEDIATION	*Objective: Take actions to stop the malicious behavior.*
1. If the system has been compromised:	
a. Temporarily remove all accesses to the accounts involved in the incident.	
b. Remove all malicious files installed by the attacker.	*Preferably, this activity would be accomplished by purging ALL files and reconstituting the files from known-safe sources.* *Note that the organization may be directed to send the suspect binaries to the appropriate CSIRT, CSIRC, or US-CERT—or request help if the organization is unsure about the malware.*
2.1.8.5 RECOVERY	*Objective: Restore the system to normal operations.*
1. Reconstitute the system using known-safe sources.	*No matter how far the hacker has gone into the system and the knowledge organizations may have (or believe they have) about the compromise, if the system has been penetrated, the best practice is to reinstall the system fully **from original media** (back-up could already be infected) and apply all fixes to the newly installed system.*
2. If the system cannot be reconstituted from a known-clean source:	
a. Change ***all*** of the system's accounts passwords.	
b. Restore ***all*** files that could have been changed (Example: *svchost.exe*) by the attacker.	*This is obviously a judgment call. ALL files are likely at SOME risk on an infected system.*
3. Verify all previous steps have been completed correctly.	
4. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*

PROCEDURE	PRINCIPLE
2.1.9 UNIX INTRUSION	
2.1.9.1 PREPARATION	
1. Develop processes and procedures for providing *physical* access to suspicious systems to applicable forensic investigators.	*Physical access is preferred to remote access, since the hacker could detect an investigation of the system (by using a network sniffer for example). Physical access may be required to disconnect the suspected machine from the network.*
2. Develop a process for creating copies of affected hard disks for forensic and evidence support.	
3. Establish baseline knowledge of *normal* network activity of assets within the applicable infrastructure.	*Organizations should maintain records describing the usual port activity to compare to the current (abnormal?) state.*
4. Establish baseline knowledge of the *normal* services running on assets within the applicable infrastructure.	*Baseline configuration standards become extremely helpful here. In addition, applicable System Security Plans should accurately show deviations from approved baselines.* *The more information that is available on an asset's "clean state", the higher the success rate in detecting unusual/abnormal activity.*
5. Establish and maintain a regularly updated list of all critical files, (especially SUID and GUID files) stored in a secure place, off of the network, or even on paper.	*With this list, administrators can easily separate usual SUID files and detect unusual ones.* *Cryptographic Hashes (MD5) of these files are a good way to efficiently manage the integrity of these critical files.*
6. Establish and maintain a map of usual port and Unix socket activity/traffic rules.	*Unix Sockets complement network port activity information.*
7. Establish and maintain a whitelist of known-good system hooks.	*Hooks speed initial assessment and subsequent malware analysis.*

PROCEDURE	PRINCIPLE
2.1.9.2 IDENTIFICATION	
CAUTION: **A Rootkit may change the results for many of the command-line steps in this procedure. Administrators should be aware that the readings they are observing might not be indicative of *actual* conditions.**	
1. Look for unusual *account* activity:	
a. Look for any suspicious entry in */etc/passwd*, especially with *UID 0*.	*Also, check /etc/group and /etc/shadow.*
b. Look for orphaned files, which could have been left by a deleted account used in the attack.	*Use # find / \(-nouser –o –nogroup \) -print.*
2. Look for unusual file activity:	
a. Look for all SUID and GUID files.	*Use # find / -uid 0 \(–perm -4000 –o –perm 2000 \) –print.*
b. Look for unusual file names, starting with ". ", ".. " , or " "	*# find / -name " *" –print* *# find / -name ". *" –print* *# find / -name ".. *" –print.*
c. Look for large files (larger than 10 MB).	*# find / -size +10 MB –print.*
d. Look for processes running from, or to, files that have been *unlinked*.	*# lsof +L1*
e. Look for unusual files in */proc* and */tmp*.	*These directories are common places for hackers to store data or malicious binaries.*

PROCEDURE	PRINCIPLE
3. Look for unusual *services* activity:	
a. For Linux only, run *chkconfig* (if installed) to check for all enabled services.	*# chkconfig --list.*
b. Verify *init* system integrity:	
(1) If the system uses System-V style *init*, verify that the standard *runlevels* and associated scripts for the system(s) have not been altered and the default *runlevel* is correct.	*Unix* init *system implementations are very platform specific within the larger "styles" of* init. *Please refer to vendor documentation and any applicable baselines or operations manuals that may detail the system specific implementations in the environment being investigated.*
(2) If the system uses BSD-style *init*, verify that the system's *rc* scripts have not been altered.	
(3) If the system uses *launchd* instead of *init* (OS X), verify the contents and integrity of the system's *launchd* scripts.	*OS X launchd scripts should be checked in:* */Library/LaunchAgents* */Library/LaunchDaemons* */Users/<user>/Library/LaunchAgents* */Users/<user>/Library/LaunchDaemons*
4. Look at the running processes.	*# ps –aux* *Use lsof –p [pid] on unknown processes. Organizations should know, and document, the usual running processes, and be able to determine which processes may have been added by an intruder. Administrators should pay special attention to the processes running under UID 0.*
5. Look for unusual network activity:	
a. Try to detect sniffers on the network using several ways:	
(1) Look at kernel log files for interfaces entering promiscuous mod.	*Such as: "kernel: device eth0 entered promiscuous mode".*
(2) Use *# ip link* to detect the *"PROMISC"* flag.	*Prefer this method to ifconfig, since ifconfig does not work on all kernels.*
b. Look for unusual port activity.	*Use: # netstat –nap and # lsof –i to get more information about processes listening to ports.*

PROCEDURE	PRINCIPLE
c. Look for unusual MAC entries in the LAN.	*# arp -a.*
d. Look for any unexpected IP address on the network.	
6. Look for unusual automated tasks:	
a. Look for unusual jobs scheduled by users mentioned in */etc/cron.allow.*	*Pay a special attention to the cron jobs scheduled by UID 0 accounts (root):* *# crontab –u root -l.*
b. Look for unusual system-wide *cron* jobs.	*# cat /etc/crontab and # ls –la /etc/cron.**
7. Look for unusual log entries.	*To look through the log files, tools like cat and grep may be useful: cat /var/log/httpd/ access.log | grep "GET /signup.jsp"*
a. Look through the log files on the system for suspicious events, including the following:	*Almost all log files are located under /var/log directory in most Linux distributions. Here are the main ones:* */var/log/message: General message and system related stuff* */var/log/auth.log: Authentication logs* */var/log/kern.log: Kernel logs* */var/log/cron.log: Crond logs (cron job)* */var/log/maillog: Mail server logs* */var/log/httpd/: Apache access and error logs directory* */var/log/boot.log: System boot log* */var/log/mysqld.log: MySQL database server log file* */var/log/secure: Authentication log* */var/log/utmp or /var/log/wtmp: Login records file.*
(1) Large number of authentication/ login failures from local or remote access tools (sshd, ftpd, etc.)	

PROCEDURE	PRINCIPLE
(2) Remote Procedure Call (RPC) programs with a log entry that includes a large number of strange characters.	
(3) A huge number of Apache logs mentioning "error".	
(4) Reboots (Hardware reboot).	
(5) Restart of applications (Software reboot).	
8. Look for unusual Kernel log entries:	
a. Look through the kernel log files on the system for suspicious events.	*Use: # dmesg* *List all important kernel and system information* *# lsmod* *# lspci.*
b. Look for known rootkits.	*Use rkhunter and other comparable tools.*
9. Check file hashes:	*Verify all MD5 hashes of binaries in /bin, /sbin, /usr/bin, /usr/sbin or any other related binary storing place. Use AIDE or comparable tools.*
WARNING: **This operation will probably change all file timestamps. This should only be done after all other investigations are complete and management approves of altering these data.**	*Management approval should be received via the CMS CSIRT (or higher) authority.*
a. On systems with RPM installed, use: *# rpm –Va | sort.*	
b. On some Linux systems, a script named *check-packages* can be used.	
c. On Solaris: *# pkg_chk –vn.*	
d. On Debian: *debsums –ac.*	

PROCEDURE	PRINCIPLE
2.1.9.3 CONTAINMENT	*Objective: Mitigate the attack's effects on the targeted environment.*
1. If the machine is considered mission essential and cannot be disconnected, perform the following:	*Most machines are NOT mission-essential. Any that are, should be identified clearly in the SSP and the CP, and appropriate actions should already be pre-identified for this specific scenario.*
a. Backup all important data in case the hacker notices the ongoing investigation and starts deleting files.	*Also, make a copy of the system's memory (RAM) for further analysis.*
2. If the machine is not considered mission-essential, perform the following.	
a. Shut the machine down by removing its power plug.	*If it is a laptop with a battery on, just push the "off" button for some seconds until the computer switches off.*
3. Start offline investigations immediately if the live analysis did not give any result.	*The system should still be considered compromised until proven otherwise.*
4. Make a copy (bit by bit) of the whole hard disk on an external storage media.	
5. Try to find evidence of every action of the hacker:	
a. Find all files used by the attacker.	*This should include deleted files (use forensic tools) to see what has been done with them or their functionality, in order to evaluate the threat.*
b. Check all files accessed recently.	
c. Inspect network shares to see if the malware has spread through it.	
d. Determine how the attacker gained access to the system.	*All leads should be considered. If no computer proof of the intrusion is found, consider whether it could come from a physical access or a complicit/stealing of information from an employee/contractor.*

PROCEDURE	PRINCIPLE
2.1.9.4 REMEDIATION	*Objective: Take action to stop the malicious behavior.*
1. If the system has been compromised:	
a. Temporarily remove all accesses to the accounts involved in the incident.	
b. Remove all malicious files installed by the attacker.	*Preferably, this activity would be accomplished by purging ALL files and reconstituting the files from known-safe sources.*
2.1.9.5 RECOVERY	*Objective: Restore the system to normal operations.*
1. Reconstitute the system using known-safe sources.	*No matter how far the hacker has gone into the system and the knowledge organizations might have (or believe they have) about the compromise, if the system has been penetrated, the best practice is to reinstall the system fully from original media and apply all fixes to the newly installed system.*
2. If the system cannot be reconstituted from a known-clean source:	
a. Change ***all*** of the system's accounts passwords.	
b. Restore ***all*** files that could have been changed by the attacker.	*This is obviously a judgment call. ALL files are likely at SOME risk on an infected system.*
c. Check the integrity of the system using MD5 hashes.	
d. Restore all binaries that could have been changed.	*Example: /bin/su.*
3. Verify all previous steps have been completed correctly.	
4. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*

PROCEDURE	PRINCIPLE
2.1.10 DENIAL OF SERVICE (DOS)	
2.1.10.1 PREPARATION	*The* Preparation *phase is considered as the most important element of a successful DoS incident response.*
1. As part of the Contingency planning[2] process:	
a. For the ISP:	
(1) Coordinate with the ISP to understand the DoS mitigation services it offers (*free* and *paid*) and what process the organization should follow to maximize their effectiveness.	
(2) Arrange for redundant Internet connection(s).	
(3) Establish contacts with the ISP and law enforcement entities.	*Make sure that the organization has the capability to use an out-of-band communication channel (e.g., phone).*
b. For the system assets:	
(1) Create a whitelist of the IP addresses and protocols the organization must allow if prioritizing traffic during an attack.	*Don't forget to include critical consumers (beneficiaries/providers, etc.), key partners, etc.*
(2) Document the IT infrastructure details, including Business Owners, IP addresses and circuit IDs, routing settings (autonomous systems, etc.)	*This should be an integral part of the SSP for the applicable system.*
(3) Prepare a network topology diagram and an asset inventory.	*This should be an integral part of the SSP for the applicable system.*

[2] Learn more about DoS attacks, and how organizations can plan for them at the SANs Institute http://www.sans.org/reading_room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi_33764.

PROCEDURE	PRINCIPLE
c. For the network infrastructure:	
(1) Design a good network infrastructure without single points-of-failure or bottlenecks.	
(2) Distribute DNS servers and other critical services (SMTP, etc.) through different autonomous systems.	
(3) Harden the configuration of network, OS, and application components that may be targeted by DoS.	
(4) Baseline the current infrastructure's performance, so administrators can identify the attack faster and more accurately.	
(5) If the CMS business is Internet dependent, implement specialized DoS mitigation products or services.	
(6) Confirm DNS time-to-live (TTL)[3] settings for the systems that might be attacked.	*Lower the TTLs, if necessary, to facilitate DNS redirection if the original IP addresses are attacked (about 600 is a good TTL value to start.)*
(7) Depending of the criticality of organizational services, consider setting-up a backup that can be easily switched to in emergencies.	
d. For internal contacts:	
(1) Establish contacts for the IDS, firewall, systems, and network teams.	
(2) Collaborate with the business lines to understand business implications (e.g., money loss) of likely DoS attack scenarios.	

[3] Time-to-live (TTL) is mechanism that limits the lifespan of data in a computer or network. Shorter TTLs can cause heavier loads on an authoritative nameserver. A TTL value 600 equates to 5 minutes. An older common TTL value for DNS was 86400 seconds, which is 24 hours, would mean that, if a DNS record was changed, DNS servers around the world could still be showing the old value from their cache for up to 24 hours after the change. TTL values are "per record" and setting this value on specific records is normally honored automatically by all standard DNS systems worldwide.

PROCEDURE	PRINCIPLE
(3) Involve the BCP/DR planning team on DoS incidents.	
2.1.10.2 IDENTIFICATION	*Objective: Detect the incident, determine its scope, and involve the appropriate parties.*
1. Analyze the attack:	
a. Understand the logical flow of the DoS attack and identify the infrastructure components affected by it.	
b. Understand if the system is the *target* of the attack or a *collateral victim*.	
c. Review the load and log files of servers, routers, firewalls, applications, and other affected infrastructure.	
d. Identify what aspects of the DoS traffic differentiate it from benign traffic.	*Examples:* *- Source IP addresses, autonomous systems, etc.* *- Destination ports* *-URLs* *-Protocols flags.*
e. Network analysis tools can be used to review the traffic.	*Tcpdump, Tshark, Snort, Argus, Ntop, Aguri, MRTG, etc.*
f. If possible, create a NIDS signature whose focus is to differentiate between benign and malicious traffic.	
2. Involve internal and external actors:	
a. Contact applicable internal teams to learn about their visibility into the attack.	
b. Contact the applicable ISP to ask for help.	*Be specific about the traffic to control:* *- Network blocks involved* *-Source IP addresses* *-Protocols.*

PROCEDURE	PRINCIPLE
c. Notify the organization's executive and legal teams.	*This includes the CMS Business Owners and the CMS CSIRT (the CSIRT will handle CMS legal notifications)—however, it may also include contractor-organization senior management.*
3. Check the background:	
a. Find out whether the organization received an extortion demand as a precursor to the attack.	
b. CMS contractors should determine if organizations or individuals would have any interest in threatening the company.	*- Competitors* *- Ideologically-motivated groups (hacktivists)* *- Former employees.*
2.1.10.3 CONTAINMENT	*Objective: Mitigate the attack's effects on the targeted environment.*
1. If the bottleneck is a particular feature of an application, temporarily disable that feature.	*If the bottleneck is at the ISP's side, only the ISP can take efficient actions. In that case, work closely with the applicable ISP and make sure that information is shared efficiently.*
2. Attempt to throttle or block DoS traffic as close to the network's *"cloud"* as possible via a router, firewall, load balancer, specialized device, etc.	*"Close to the cloud" means as close to the network's external or untrusted network connection that is the source of the attack.*
3. Terminate unwanted connections or processes on servers and routers and *tune* their TCP/IP settings.	*TCP tuning techniques adjust the network congestion-avoidance parameters of TCP connections.*
4. If possible, switch to alternate sites or networks using DNS or another mechanism.	*Blackhole DoS traffic targeting the original IP addresses.*
5. Set up an alternate communication channel with users (e.g., web server, mail server, voice server, etc.)	
6. If possible, route traffic through a traffic-scrubbing service or product via DNS or routing changes (e.g., *sinkhole* routing).	

PROCEDURE	PRINCIPLE
7. Configure egress filters to block traffic internal systems may be sending in response to DoS traffic (e.g., *backscatter* traffic), to avoid adding unnecessary packets to the network.	
8. In case of an extortion attempt, try to buy time with the fraudster.	*For example, explain that the organization needs more time in order to get management approval.*
2.1.10.4 REMEDIATION	*Objective: Take actions to stop the Denial of Service condition.* *Technical remediation actions can mostly be enforced by the applicable ISP.*
1. Contact the applicable ISP resources and make sure that it properly enforces remediation measures.	*For information, here are some of the possible measures:* *- Filtering (if possible at level Tier 1 or 2)* *- Traffic-scrubbing/Sinkhole/Clean-pipe* *- Blackhole Routing.*
2. If the DoS sponsors have been identified, consider involving law enforcement.	*This should be performed upon the direction of CMS and the applicable contractor's executive and legal teams.*
2.1.10.5 RECOVERY	*Objective: Restore the system to normal operations.*
NOTE: **Ensure that the recovery-related actions are decided in accordance with the appropriate network teams. Bringing up services could have unexpected side effects.**	
1. Assess the end of the DoS condition:	
a. Ensure that the impacted services are *reachable* again.	
b. Ensure that the infrastructure performance is back to established baseline performance levels.	
2. Rollback applied mitigation measures:	
a. Switch traffic back to the original network.	

PROCEDURE	PRINCIPLE
b. Restart stopped services.	
3. Verify all previous steps have been completed correctly.	
4. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*
2.1.11 MALICIOUS NETWORK BEHAVIOR	
2.1.11.1 PREPARATION	*Objective: Establish contacts, define procedures, gather information, and get familiar with intrusion detection tools to save time during an attack.*
1. Intrusion detection systems (IDS):	
a. Ensure that the monitoring tools are up to date.	
b. Establish contacts with the organization's and CMS' network and security operation teams.	
c. Make sure that an alert notification process is defined and well known by everyone.	
2. Network:	
a. Make sure that an inventory of the network access points is available and up-to-date.	
b. Make sure that network teams have up to date network maps and configurations.	
c. Look for potential unwanted network access points (xDSL, Wi-Fi, Modem, etc.) regularly and close them.	
d. Ensure that traffic management tools and processes are operational.	

PROCEDURE	PRINCIPLE
3. Baseline traffic: a. Identify the baseline traffic and flows. b. Identify the business-critical flows.	
2.1.11.2 IDENTIFICATION	*Objective: Detect the incident, determine its scope, and involve the appropriate parties.*
1. Sources of detection: a. Notification by user/helpdesk. b. IDS alert. c. Detection by network staff. d. Complain from an external source. e. SOC alert.	
NOTE: **Network forensics requires skills and knowledge. Coordinate with the CSIRT for assistance or advice.**	*The CMS CSIRT will coordinate with the CSIRC and the US-CERT to identify resources and expertise.*
2. Record suspected network activity.	*Network frames can be stored into a file and transmitted to the applicable team (CSIRT, CSIRC, US-CERT) for further analysis.* *Use network capture tools (tshark, windump, tcpdump…) to dump malicious traffic. Use a hub or port mirroring on an affected LAN to collect valuable data.*
3. Analyze the attack: a. Analyze alerts generated *Intrusion Detection Systems.* b. Review statistics and logs of network devices. c. Try to understand the goal of the malicious traffic and identify the infrastructure components affected by it.	

PROCEDURE	PRINCIPLE
d. Identify the technical characteristics of the traffic.	*Evaluate:* *- Source IP address(es)* *- Ports used, TTL, Packet ID* *-Protocols used* *- Targeted machines/services* *- Exploit(s)* *- Remote accounts logged in.*
2.1.11.3 CONTAINMENT	*Objective: Mitigate the attack effects on the neighboring IT resources.*
NOTE: **If the issue is targeting specific PII/PHI resources, immediately notify the CMS Breach Analysis Team (BAT).**	
1. Depending on the criticality of the impacted resources, the following steps can be performed and monitored :	
a. Disconnect the compromised area from the network.	
b. Isolate the source of the attack. Disconnect the affected computer(s) in order to perform further investigation.	
c. Find acceptable mitigation measures for the business-critical traffic in agreement with the business line managers.	
d. Terminate unwanted connections or processes on affected machines.	
e. Use firewall/IPS rules to block the attack.	
f. Use IDS rules to match with this malicious behavior and inform technical staff on new events.	
g. Apply ad hoc actions in case of strategic issue:	
(1) Block exfiltration destination or remote location on Internet filters.	

PROCEDURE	PRINCIPLE
(2) Restrict strategic file servers to reject connections from the compromised computer.	
(3) Select what kind of files can be lost/ stolen and restrict the access for confidential files.	
(4) Create fake documents with watermarking that could be used as a proof of theft.	
(5) Notify targeted business users about what must be done and what is forbidden.	
(6) Configure logging capabilities in verbose mode on targeted environment and store them in a remote secure server.	
2.1.11.4 REMEDIATION	*Objective: Take actions to stop the malicious behavior.*
1. Block the source:	
a. Using analysis from previous steps, find all communication channels used by the attacker and block them at network boundaries.	
b. If the source has been identified as an insider, take appropriate actions and involve applicable management and/or Human Resources team and/or legal team.	
c. If the source has been identified as an external offender, consider involving abuse teams and law enforcement services if required.	
2. Technical remediation:	
a. Define a remediation process.	*If necessary, this process can be validated by another organizational structure, such as the local Incident Response Team.*
b. Remediation steps from applicable *Intrusion* procedures may also be useful.	
(1) For *Windows Intrusions*, perform applicable actions in Section 2.1.8.	

PROCEDURE	PRINCIPLE
(2) For *Unix Intrusions*, perform applicable actions in Section 2.1.9.	
3. Test and enforce:	
a. Test the remediation process and make sure that it properly works without damaging any service.	
b. Enforce the remediation process once tests have been approved by both IT and business.	
2.1.11.5 RECOVERY	*Objective: Restore the system to normal operations.*
1. Verify all previous steps have been completed correctly.	
2. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*
2.1.12 WEBSITE DEFACEMENT	
2.1.12.1 PREPARATION	*Objective: Establish contacts, define procedures, and gather information to save time during an attack.*
1. Have up-to-date schemes describing applicative components related to web servers.	
2. Build backup websites, upon which the organization can publish content during emergencies.	
3. Define a procedure to redirect every visitor to this backup website.	
4. Deploy monitoring tools to quickly detect any abnormal behavior on applicable websites.	
5. Export the web server's log files to an external server. Make sure clocks are synchronized between each server.	

PROCEDURE	PRINCIPLE
6. Reference external contents (static or dynamic) and create a list for each of them. Do not forget third parties for advertisement.	
7. Reference contact points of the hosting provider/environment.	
8. Ensure the hosting provider/environment enforces policies to log all events.	
9. Maintain an up-to-date network map.	
2.1.12.2 IDENTIFICATION	*Objective: Detect the incident, determine its scope, and involve the appropriate parties.*
1. Usual channels of detection are:	
a. Webpage monitoring: The content of a web page has been altered.	*The new content is either very discreet (an "iframe" injection for example) or obvious ("You have been 0wn3d by xxx").*
b. Users call or notification from employees about problems they noticed while browsing the website.	
c. Security checks with tools.	*Such as Google* SafeBrowsing[4] *or other comparable tools.*
NOTE: **The source code of the suspicious page must be analyzed carefully to clearly identify the problem. In particular, be sure the problem is on a web server belonging to the organization and *not* on a web content located outside of the CMS/contractor infrastructure (like third-party banners.)**	
2. Verify the defacement and detect its origin:	
a. Check files with static content (in particular, check the modification dates, hash signature).	

[4] Google's *SafeBrowsing* tool provides a quick review of the history of a specific site over the last 90 days. To determine the history, submit a URL such as http://www.google.com/safebrowsing/diagnostic?site=CMS.HHS.gov, referencing the applicable site address to be validated.

PROCEDURE	PRINCIPLE
b. Check *mashup* content providers.	
c. Check links present in the web page.	*src, meta, ccs, script, etc.*
d. Check log files.	
e. Scan the databases for malicious content.	
2.1.12.3 CONTAINMENT	*Objective: Mitigate the attack's effects on the targeted environment.*
1. Backup all data stored on the web server for forensic purposes and evidence collecting.	*The best practice here, if applicable, is to make a complete bit-by-bit copy of the hard disk containing the web server. This will be helpful to recover deleted files.*
2. Verify that the vulnerability exploited by the attacker is not located somewhere else.	
3. Check the system on which the web server is running.	
4. Check other services running on that machine.	
5. Check the connections to other systems that might be compromised.	
6. If the source of the attack is another system on the network, disconnect it if possible physically and investigate it.	
7. Find out how the attacker got into the system in the first place.	
8. Web component vulnerability allowing write access.	*Fix any vulnerability by applying editor's fix.*
9. Open public folder.	
10. SQL weakness allowing injection.	
11. Mashup components.	
12. Administrative modification by physical access.	

PROCEDURE	PRINCIPLE
13. If required for complex issues and mission-essential web servers, deploy a temporary web server, up to date with applicable applications.	*The temporary web server should offer the same content than the compromised web server, or at least show other legitimate content such as "Temporary unavailable". The best is to display a temporary static content, containing only HTML code. This prevents another infection in case the attacker has used vulnerability in the legitimate PHP/ ASP/CGI/PL/etc. code.*
2.1.12.4 REMEDIATION	*Objective: Take actions to remove the threat and avoid future defacements.*
1. Remove all altered content and replace it with the legitimate content, restored from earlier backup.	*Make sure this content is free from vulnerabilities.*
2.1.12.5 RECOVERY	*Objective: Restore the system to normal operations.*
1. If the web server provides user-authentication:	
a. If there is indication *or suspicion* that passwords may have been compromised, ***change all user passwords***.	*This can require a large user communication.*
2. If a backup web server has been used:	
a. Restore the primary web server component.	
3. If the defacement has been visible to the public, create a communications plan to explain the incident publicly.	
4. Verify all previous steps have been completed correctly.	
5. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*

PROCEDURE	PRINCIPLE
2.1.13 BLACKMAIL	*Objective: Establish contacts, define procedures, and gather information to save time during an attack.*
2.1.13.1 PREPARATION	
1. Establish appropriate POCs: a. Identify internal contacts (security team, incident response team, legal department, etc.) b. Identify external contacts that might be needed, mainly for investigation purposes like Law Enforcement. c. Make sure that the security incident escalation process is established and the actors are clearly defined. d. Be sure to have intelligence gathering capabilities (communities, contact, etc.) that might be involved in such incidents.	
2. Make sure that all the relevant employees are aware of blackmail issues.	*This can be part of the security awareness program.*
2.1.13.2 IDENTIFICATION	*Objective: Detect the incident, determine its scope, and involve the appropriate parties.*
1. Alert relevant people.	
2. Keep traces of any communications related to the incident.	*Do not send emails to trash; write down any phone contact with phone number and timestamp if available, fax, etc. Try to get as many details as possible about the author (name, fax, postal address, etc.)*
3. Examine possible courses of actions with applicable incident response teams and legal teams.	*Different Government and contractor organization may have specific policies and procedures to address this threat.*
4. If sensitive CMS information is concerned, verify a safe backup and determine how it was compromised.	

PROCEDURE	PRINCIPLE
5. Include top management to inform them that blackmail is happening and is being handled according to a defined process.	
2.1.13.3 CONTAINMENT	*Mitigate the attack's effects on the targeted environment.*
1. Determine how the organization can respond to the blackmail.	*The organization should weigh the consequences and costs of: 1) Ignoring, 2) answering Yes, or 3) answering No.*
2. Most common threats tied with blackmail are:	
a. Denial of service.	
b. Reveal sensitive data on Internet (Federal PII, PHI, or internal worker/director information, confidential contractor data, etc.)	
c. Reveal sensitive private information about employees/VIPs.	
d. Block data access (wiped or encrypted through *ransomware* for example).	
e. Mass-mailing using the brand (spam, child pornography, bad rumors, etc.)	
3. Check the background:	
a. Check if similar blackmail attempts have taken place in the past. Check if other companies have been threatened as well.	
b. All related technical data should be checked carefully and collected for investigation purposes.	
c. CMS contractors should determine if organizations or individuals would have any interest in threatening the company.	*- Competitors* *- Ideologically-motivated groups (hacktivists)* *- Former employees.*
d. Try to identify the attacker with the available pieces of information.	

PROCEDURE	PRINCIPLE
e. More generally, try to find how the attacker got into the system or got the object of the blackmail.	
4. Contact local law enforcement to inform them.	*If the organization does not wish to file a complaint, at least notify Law Enforcement as other organizations could be affected. At the same time, inform hierarchy and subsidiaries to have a unique position in case the fraudster tries to blackmail another internal department.*
5. Try to gain time and details from fraudster. Ask for:	
a. Proof of what they claim: example data, intrusion proof, etc.	
b. Time to get what fraudster wants (money, etc.)	
2.1.13.4 REMEDIATION	*Objective: Take actions to remove the threat and avoid future incidents.*
1. If a flaw has been identified on a technical asset or a process allowing the attacker to get access to the object of the blackmail, ask for an IMMEDIATE fix in order to prevent another case.	
2. After getting as much information as possible, ignore the blackmail and ensure appropriate monitoring is in place to detect and react accordingly on any new follow-ups.	*Remember that a positive answer to the fraudster is an open door for further blackmail.*
3. Do not make any remediation decision alone if strategic assets or human people are targeted. Involve appropriate departments.	
2.1.13.5 RECOVERY	*Objective: Restore the system to normal operations.*
1. Notify the top management of the actions and the decision taken on the blackmail issue.	

PROCEDURE	PRINCIPLE
2. If the Blackmail has been made visible to the public, create a communications plan to explain the incident publicly.	
3. Verify all previous steps have been completed correctly.	
4. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*
2.1.14 SMARTPHONE MALWARE	*Objective: Establish contacts, define procedures, and gather information to save time during an attack.*
2.1.14.1 PREPARATION	
1. Mobile helpdesk must have a defined process in case of a suspected malware infection: replace the smartphone of the user with a new one and isolate the suspicious device for analysis by the forensic investigator.	
2. A good knowledge of the usual activity of the smartphone is appreciated (default and extra tools running on it).	*A smartphone support expert can be helpful to assist the forensic investigator.*
3. A monitoring should be done to check unusual user bill or network activity.	
2.1.14.2 IDENTIFICATION	*Objective: Detect the incident, determine its scope, and involve the appropriate parties.*
1. Main points of notification for suspicious smartphone: a. Antivirus raises alerts. b. Unusual system activity, unusually slow system. c. Unusual network activity, very slow Internet connection.	

PROCEDURE	PRINCIPLE
d. The system reboots or shutdowns without reason.	
e. Some applications crash unexpectedly.	
f. User receives one or multiple messages, some could have unusual characters (SMS, MMS, Bluetooth messages, etc.)	
g. Huge increase in phone bill or web activity.	
h. Unusual calls to unusual phone numbers or at unusual hours/days.	
2. Evidence such as website URLs need to be gathered.	
3. Ask the user about his/her usual activity on the smartphone: which websites are browsed, which external applications are installed.	*This information can optionally be crosschecked with the Agency/contractor policy.*
2.1.14.3 CONTAINMENT	*Objective: Mitigate the attack's effects on the targeted environment.*
1. Ensure user is given a temporary or new permanent device to avoid any time constraint on the investigation.	
2. Back up the smartphone data.	
3. Remove battery to block all activity (Wi-Fi, Bluetooth, etc.)	
4. Launch an antivirus check on the computers that are/have been synchronized or linked with the smartphone.	
5. If directed by the CSIRT or CSIRC, send the suspicious smartphone and appropriate components (SIM, battery, power cable, memory cards) to the applicable security incident response team.	*This team will help to isolate the malicious content and send it to antivirus companies, and possibly identify the source.*

PROCEDURE	PRINCIPLE
2.1.14.4 REMEDIATION	*Objective: Take actions to remove the threat and avoid future incidents.*
1. If some encryption or password accesses are set, find out a way to get access to the stored data.	*If this is not possible, the investigation will suffer high limitations.*
2. Specific tools should be used by the incident response team to conduct a forensic investigation on the smartphone.	*Below is a short list of tools that may be useful: XDA Utils (Windows Mobile), MIAT (Mobile Internal Acquisition Tool – Symbian, Windows Mobile), TULP2G, Blackberry Desktop Manager, XRY, Cellebrite, Paraben. However, others tools may also be available.*
3. Remove SIM from the smartphone if not already done.	
4. Recover phone history, web history and all available logs.	
5. Recover server connections log if available.	
6. Identify and remove the threat on the smartphone.	
7. If the threat is related to an installed application, identify its location on Internet and remove it.	
2.1.14.5 RECOVERY	*Objective: Restore the system to normal operations.*
1. Once the investigations are over, wipe the infected smartphone (if possible), reset it to factory settings with a pristine firmware, and file system, in order to be used again.	
2. Restore the data saved previously from a trusted source on the destination device.	
3. Verify all previous steps have been completed correctly.	
4. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*

PROCEDURE	PRINCIPLE
2.1.15 SOCIAL ENGINEERING	*Objective: Establish contacts, define procedures, and gather information to save time during an incident.*
2.1.15.1 PREPARATION	
1. Raise user awareness and security policies:	
a. Never give any personal or corporate information to an unidentified person.	*This could include user IDs, passwords, account information, name, email address, phone (mobile or landline) numbers, address, social security number, job titles, and information on clients, organization, or IT systems.*
b. The goal of the social engineer is to steal PII/PHI, human resources, corporate/agency secrets, or user data.	
c. Report any suspicious event to management, who should forward it to the CMS CSIRT.	
2. Have a defined process to redirect any *strange* request to a *"Red"* phone, if needed.	*"Red" phone number must be clearly tagged as "Social Engineering". The phone number has to be easy to identify in the global phone directory of applicable organizations but requests on reverse number should not be displayed. Red phone line should always be recorded for evidence collecting purposes.*
3. Prepare to handle a conversation with social engineers to identify which information could help tracking the attacker and his goals.	

PROCEDURE	PRINCIPLE
2.1.15.2 IDENTIFICATION	*Objective: Detect the incident, determine its scope, and involve the appropriate parties.*
1. User Actions:	
a. Phone Call:	*Some unknown caller calls, asking for detailed information.*
(1) If the contact call from a non-CMS organization, requests for information that could be valuable, deny the requests and proceed to *Containment* procedures in Section 2.1.15.3.	
(2) If the contact pretends to be an employee, but the phone number is hidden or not internal, propose calling back to the declared number in the directory. If this option is rejected, proceed to *Containment* procedures in Section 2.1.15.3.	*The attacker might use several techniques to entice his victim to speak (fear, curiosity, empathy ...). Do not disclose information in any case.* *Listen carefully to his requests and at the end ask for a phone number to call back or an email address to reply.* *Take notes and stay calm, even if the attacker is shouting or threatening, remember he tries to use human weaknesses.*
(3) If possible, collect the following information: (a) The name of the correspondent. (b) Requested information/people. (c) Accent, language skills. (d) Industry language and organizational knowledge. (e) Background noises. (f) Time and duration of the call.	

PROCEDURE	PRINCIPLE
b. Email:	*Someone unknown requests detailed information.*
(1) If the contact has an "out of the organization" email address and requests information that could be valuable, proceed to *Containment* procedures in Section 2.1.15.3.	
(2) If the contact uses an internal email address but is asking for unusual information, ask for further explanation and use the organizational directory to "copy" the appropriate manager.	
2. Notify top management to inform them that an incident has been encountered relating to a social engineering attack.	*Upper management may have better understanding of the strategic goals of the attack (the target information) based on the context.*
2.1.15.3 CONTAINMENT	*Objective: Mitigate the attack's effects on the targeted environment.*
1. Actions for all employees:	
a. Phone call:	
(1) If the attacker request a phone number, follow these steps:	
(a) Use the "red phone line" from the organization CERT/CSIRT, if existing.	
(b) Give him the number with an invented name.	
(c) Immediately call the applicable CERT/CSIRT team explaining what happened and the chosen invented name.	
(2) If the attacker does not give time to find the *Red Phone* number, ask them to call back later.	

PROCEDURE **PRINCIPLE**

(3) If the attacker wants to reach someone, follow these steps:

(a) Place on hold the attacker, call CERT/CSIRT team, and explain what happened.

(b) Transfer the attacker to CERT/ CSIRT team (do not give him the number).

b. Email:

(1) Forward to the CMS CSIRT all email including headers (send as attached documents) for investigation purposes.

2. IR Authority/CSIRT:

a. Phone call:

(1) Resume the conversation with the attacker and use one of these techniques:

(a) Impersonate a person to whom the attacker is willing to speak.

(b) Slow down and extend the conversation and entice the attacker to make a mistake.

(c) Explain to him that social engineering is forbidden by law, punishable by sanctions and that the legal team will handle the issue if it continues.

(2) If the trap phone number has been used, prepare to "burn it", create another one and display it in the directory.

b. Email:

(1) Collect as much information as possible on the email address:

(a) Analyze the email headers and try to locate the source.

(b) Search the email address with Internet tools.

PROCEDURE	PRINCIPLE
(c) Geolocalize the user behind the email address.	
(2) Aggregate all social engineering attacks to visualize the scheme.	
2.1.15.4 REMEDIATION	*Objective: Take actions to remove the threat and avoid future incidents.*
1. Some possible remediation actions can be tried:	
a. Alert the law enforcement and/or file a complaint.	
b. Discuss the problem in circles of trust to know if the company is facing this issue alone.	
c. Threaten the attacker with legal actions if he can be identified.	
2.1.15.5 RECOVERY	*Objective: Restore the system to normal operations.*
1. Notify the top management of the actions and the decisions taken on the social engineering case.	
2. Verify all previous steps have been completed correctly.	
3. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*

PROCEDURE

2.1.16 INFORMATION LEAKAGE

2.1.16.1 PREPARATION

1. Establish contacts:

a. Identify internal technical contacts (security team, incident response team, Business Owners, etc.)

b. Make sure to have contact points in *Public Relations*, *Human Resources*, and *Legal* departments.

c. Identify external contacts that might be needed, mainly for investigation purposes (like Law Enforcement for example).

2. Develop security policy:

a. Make sure that the information *value* is explained in the policy, applicable IT charts, and awareness training sessions.

b. Make sure all *valuable* assets are properly identified in the applicable risk assessments.

c. Make sure that the security incident escalation process is established and the actors are clearly defined and identified.

PRINCIPLE

Objective: Establish contacts, define procedures, and gather information to save time during the incident handling.

PROCEDURE	PRINCIPLE
2.1.16.2 IDENTIFICATION	*Objective: Detect the incident, determine its scope, and involve the appropriate parties.*
NOTE: **Data leakage can occur from anywhere. Remember that the cause of the leakage can be an individual employee willingly or unwillingly bypassing security issues, or a compromised computer.**	
1. Detect the issue:	
a. Incident notification process.	*Internal information can be a good source of detection: employee confidence, security team identifying a problem, etc.*
b. Public monitoring tools.	*A watch on Internet search engines and public database can be very valuable to detect information leakage.*
c. Data Loss Detection/Prevention (DLD/ DLP) tools.	*If there is a DLD/DLP tool in the company, it can provide valuable information to incident handlers working on information leakage.*

PROCEDURE	PRINCIPLE
2. Confirm the issue:	
WARNING: **Do *NOT* take any actions without approval from the CMS CISO.**	*There are several legal issues to be resolved before* some *actions can be taken. CMS CSIRT will coordinate with the CSIRC, US-CERT, and appropriate legal resources, as applicable.*
NOTE: **Consider ALL of the paths for data leakage, even when evidence has been already found at a particular path. Proof of other methods of data leakage may also be present.**	*Also, do not forget that someone else could have accessed the computer. Was the suspected employee actually in front of his computer when the leak occurred?*
a. If the detected leakage occurred via Email:	
(1) If the disclosure source was a corporate/government email address:	
(a) On the messaging system, look for emails sent to or received from a suspect account or with a special subject.	
(b) On the email client on the desktop of the suspect (if available), use a tool which allows searching by filtering out the "PRIVATE" flagged emails.	
(c) When applicable, look through related log files.	
(2) Use forensic tools to check for deleted browsing history.	*Also, check all the offline content left from all browsing.*
b. If the detected leakage occurred via Browsing:	*Data might have been sent on webmail/ forums/dedicated websites.*
(1) On the proxy server, check the logs relating to the suspect account connections on the suspected URL used to disclose data.	

PROCEDURE	PRINCIPLE
(2) On the desktop (if available), check the history of the installed browsers.	*Remember some people might have different browsers on the same desktop computer; be sure to check every browser history. If the moment of the data leak can be time-stamped, some log files can provide useful information.*
c. If the detected leakage occurred via external storage devices:	*A various number of devices can be used to store data: USB keys, CD-ROM, DVD, external hard disks, smartphones, memory cards…*
(1) Little information will be found concerning data transfer using these devices.	*The USB key used to transfer data can be referenced by the operating system. A forensic analysis can confirm the use of hardware but not the data transmitted.*
d. If the detected leakage occurred via local files:	*If nothing has been found yet, there are still chances to find traces in the local file system of the suspect.*
(1) Use a parsing tool that forbids any access to the PRIVATE zone of the user.	*Act accordingly to local employment law.*
e. If the detected leakage occurred via network transfer:	*Multiple ways might be used to transfer data out of the company: FTP, instant messenger, etc.*
(1) Try to dig into log files showing such activity.	
(2) Data might also have been sent using a VPN tunnel or on an SSH server.	*In this case, one can prove the connection by watching log files but cannot see the content transmitted.*
f. If the detected leakage occurred via a printer:	*Data can be sent to printers connected to the network.*
(1) Check for traces on the spooler or directly on the printer.	*Some constructors directly store printed documents on a local hard drive.*
g. If the detected leakage occurred via malware:	
(1) If nothing has been found, think of a possible *malware* compromise and act accordingly with the "Malware Detection" procedure.	

PROCEDURE	PRINCIPLE
2.1.16.3 CONTAINMENT	*Objective: Mitigate the attack's effects on the targeted environment.*
1. Notify the management, legal, and PR team to make sure they are prepared to deal with a massive or targeted disclosure.	
2. Depending on the leakage vector, block the access to the disclosure URL, the disclosure server, the disclosure source, or the disclosure recipients.	*This action must be done on all infrastructure points.*
3. Suspend the logical and physical credentials of the insider if the leakage has been confirmed.	*Involve Human Resources and legal team before any action.*
4. Isolate the computing system (desktop, printer) used to disclose data in order to perform a forensic analysis later.	*This manipulation should be done the hard way: remove the electric plug (and the battery in case of a laptop).*
2.1.16.4 REMEDIATION	*Objective: Take actions to remove the threat and avoid future incidents.*
1. If data has been sent to public servers, ask the owner (or webmaster) to remove the disclosed data.	*Be sure to tailor the request to the recipients (*hacktivism *webmaster will not behave as a* press *webmaster).*
2. If it is not possible to remove the disclosed data, provide a complete analysis to the PR team and the management.	*Monitor leaked documents spread on websites and social networks (Facebook, Twitter, etc.) and Internet user's comments or reactions.*
3. Provide the elements to the Human Resources tea.	*This information may be needed to file a complaint against a suspected "insider."*
2.1.16.5 RECOVERY	*Objective: Restore the system to normal operations.*
1. If a system has been compromised, restore it completely.	
2. Warn employees (or applicable local teams) about the issue to raise awareness, and re-enforce or update security rules.	
3. When situation stabilizes, remove the official communication.	

PROCEDURE	PRINCIPLE
4. Verify all previous steps have been completed correctly.	
5. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*
2.1.17 INSIDER ABUSE	
2.1.17.1 PREPARATION	*Objective: Establish contacts, define procedures, and gather information to save time during the incident handling.*
1. Establish Points of Contact:	
a. Make sure to also have contact points in *Public Relations*, *Human Resources*, and *Legal* departments.	
b. Have a centralized logging facility.	
c. Be sure to have a global authorization and clearance process.	*This process must specially take care of the removal of privileges on former jobs.*
2. Provide strong authentication according to the appropriate IA requirements of the ARS.	
2.1.17.2 IDENTIFICATION	*Objective: Detect the incident, determine its scope, and involve the appropriate parties.*
NOTE: **Insider abuses are hard to detect and there are no 100 percent effective methodologies.**	
1. Technical Identification:	
a. Alerts from a SIEM or correlation tools.	*Malicious behavior can have been detected with the correlation of several abnormal events.*
b. Alerts from an IDS/IPS detecting an intrusion.	*In case the insider tried to hack the system, an Intrusion Detection System (or Intrusion Prevention System) can be able to trigger an alert.*

PROCEDURE	PRINCIPLE
2. Human identification:	
a. Management.	*The manager of the insider might be the first to notice the suspected behavior.*
b. Control, risk, compliance.	*These teams have their own systems to detect operational anomalies and they can trigger alerts if something abnormal is detected.*
c. Colleagues.	*Insider's colleagues are maybe the most valuable notification channel because they know perfectly the tasks, the process, and the impacts on their duty jobs. They can guess easily what is happening.*
d. External parties.	*External partners or structure can also have their own detection capabilities. If operations have been falsified internally, these external entities can bring a real enlightenment.*
2.1.17.3 CONTAINMENT	*Objective: Mitigate the attack's effects on the targeted environment.*
WARNING: **Do NOT take any actions without approval from the CMS CISO.**	
1. Involve appropriate personnel.	*Different people should be informed about the abuse so that they can help to assist on it. This includes Human Resources management, legal management, PR management and business management of the suspected insider.*
2. Meet with the suspected insider.	*A Human Resources manager should meet the suspected insider to explain him/her what has been found and what will happen. Support can be required from legal, technical and management people.*
3. Lower privileges.	*If the suspected insider is allowed to stay at work until the end of the investigation, provide him/her a computer with minimum authorizations.*

PROCEDURE	PRINCIPLE
4. Freeze access and authorizations.	*Suspend access and authorizations of the suspected insider. This must include application clearance. This can also include system account, keys, building facility badge.*
5. Suspend remote access.	*Suspend remote access capabilities, (i.e., smartphones, VPN accounts, tokens...)*
6. Seize corporate/federal computing devices.	*Seize all the professional computing device of the suspected insider.*
7. In the case of *abnormal* activity:	*Nothing malicious or fraudulent is confirmed yet.*
a. Initiate forensics investigation on the computing devices of the suspected insider.	
b. Initiate log investigations on different audit trail components.	
8. In the case of confirmed malicious or fraudulent activity:	
a. In this case, do not take any further technical actions. Provide the legal team or law enforcement official all requested evidences and be ready to assist on demand.	
9. If collateral damages can result from the abuse, be sure to contain the incident impacts before making it public.	*Be sure to inform authorities if required.*
2.1.17.4 REMEDIATION	*Objective: Take actions to remove the threat and avoid future incidents.*
NOTE: **Remediation is limited in case of an insider abuse.**	
1. Take disciplinary action against the malicious employee (or terminate the contract) and remove all his/her credentials.	
2. Delete all fictitious or fraudulent operations made by the insider.	

PROCEDURE	PRINCIPLE
3. Review all programs or scripts made by the insider and remove all unnecessary codes.	
2.1.17.5 RECOVERY	*Objective: Restore the system to normal operations.*
1. If the incident has not been made public yet, be sure to warn all the impacted stakeholders (employees, business partners, other CMS contractors, concerned partners …) and required authorities.	*This communication must be made by top management in case of huge impacts.*
2. Eventually warn employees or some local teams about the issue to raise awareness and increase security rules.	
3. Verify all previous steps have been completed correctly.	
4. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*
2.1.18 PHISHING	
2.1.18.1 PREPARATION	*Objective: Establish contacts, define procedures, and gather information to save time during an attack.*
1. Create a list of all legitimate domains belonging to the organization.	*This will help analyzing the situation, and prevent starting a takedown procedure on a "forgotten" legitimate website.*
2. Prepare a web page hosted on organizational infrastructure, to be ready to warn of an ongoing phishing attack.	*Prepare and test a clear deployment procedure as well.*
3. Prepare takedown email forms.	*These will be necessary for every phishing case, if possible in several languages. This will speed up things when trying to reach the hosting company etc. during the takedown process.*

PROCEDURE	PRINCIPLE
4. Establish internal contacts:	
a. Maintain a list of all people involved in domain names registration in the organization.	
b. Maintain a list of all people authorized to make decisions on cybercrime and eventual actions regarding phishing.	
5. Establish external contacts:	
a. Have several ways to be reached in a timely manner (24/7 if possible):	
(1) Email address, easy to remember for everyone (ex: security@yourcompany).	*CMS internal organizations should use CISO@cms.hhs.gov.*
(2) Web forms on an organizational website.	*Location of the form is important. It should ideally be no more than two clicks away from the* Main *page.*
(3) Visible *Twitter* account.	
b. Establish and maintain a list of takedown contacts in:	
(1) Hosting companies.	
(2) Registry companies.	
(3) Email providers.	
c. Establish and maintain contacts in CERTs, they will probably always be able to help if needed.	*CSIRT, CSIRC, and US-CERT as applicable.*
6. Raise consumer awareness.	*Do not wait for phishing incidents to communicate with consumers (beneficiaries/ providers, etc.) Raise awareness about phishing fraud, explain what phishing is, and make sure consumers know CMS will never ask them for credentials/banking information by email or on the phone.*

PROCEDURE	PRINCIPLE
7. Raise business line awareness.	*People in business lines must be aware of phishing problems and consider security as a priority. Therefore, they should apply good practices such as avoid sending links (URL) to consumers (beneficiaries/providers, etc.), and use a signature stating that the company will never ask them for credential/banking or other PII/PHI online.*
2.1.18.2 IDENTIFICATION	*Objective: Detect the incident, determine its scope, and involve the appropriate parties.*
1. Monitor all points of contact closely (email, web forms, etc.)	
2. Deploy spam traps and try to gather spam from partners/third-parties.	
3. Deploy active monitoring of phishing repositories.	*Like* AA419 *or* PhishTank *for example.*
4. Monitor specialized mailing lists or RSS/ Twitter feeds which may be reporting phishing cases.	*Use automated monitoring systems on all of these sources, so that every detection triggers an alarm for instant reaction.*
5. Monitor web logs.	*Check there is no suspicious referrer bringing people to organizational websites. This is often the case when the phishing websites brings the user to the legitimate website after they have been victimized.*
6. Involve appropriate parties:	
a. As soon as a phishing website is detected, contact appropriate management officials and the CMS CISO.	
b. The decision to act on the fraudulent website/email address must be taken as soon as possible.	*As soon as possible means within minutes.*

PROCEDURE	PRINCIPLE
7. Collect evidence:	
a. Make a time-stamped copy of the phishing web pages.	*Use an efficient tool to do that, like HTTrack for example. Do not forget to take every page of the phishing scheme, not just the first one if there are several. If needed, take screenshots of the pages.*
2.1.18.3 CONTAINMENT	*Objective: Mitigate the attack's effects on the targeted environment.*
1. Spread the URL of the attack in case of a phishing website.	*This will prevent the users from accessing the website while appropriate officials work on the remediation phase.* *Use every way available to spread the fraudulent URL on every web browser: use the options of Internet Explorer, Chrome, Safari, Firefox, Netcraft toolbar, Phishing-Initiative, etc.*
2. Spread the fraudulent email content on spam-reporting websites/partners.	
3. Communicate with applicable consumers (beneficiaries/providers, etc.)	*Deploy the alert/warning page with information about the current phishing attack.* *If the organization is impacted several times a week, do not always deploy an alert/warning message, but rather a very informative phishing page to raise consumer awareness.*
4. Check the source-code of the phishing website.	
a. See where the data is exported.	*This may be to another web content that is not accessible (a PHP script usually), or sent via email to a fraudster mail drop.*
b. Watch how the phishing-page is built:	*Do the graphics come from a legitimate organizational website, or are they stored locally?*
(1) If possible, in case the graphics are taken from organizational websites, change the graphics to display a "PHISHING WEBSITE" logo on the fraudster's page.	

PROCEDURE	PRINCIPLE
2.1.18.4 REMEDIATION	*Objective: Take actions to stop the fraud.*
1. In case the fraudulent phishing pages are hosted on a compromised website, try to contact the owner of the website.	*Explain clearly the fraud to the owner, so that he takes appropriate actions: remove the fraudulent content, and most of all upgrade the security on it, so that the fraudster cannot come back using the same vulnerability.*
2. In any case, also contact the hosting company of the website.	*Send emails to the contact addresses of the hosting company (generally, there is an abuse@hostingcompany) then try to get someone on the phone, to speed things up.*
3. Contact the email hosting company to shut down the fraudulent accounts that send or receive the stolen information.	
4. In case there is a redirection (the link contained in the email often goes to a redirecting URL), also take down the redirection by contacting the company responsible for the service.	*URL-shortening services are frequently utilized to hide the destination from organizational perimeter defenses.*
5. If no action is taken, call back and send emails on a regular basis.	
6. If the takedown is too slow, contact a local CERT in the involved country for assistance.	
2.1.18.5 RECOVERY	*Objective: Restore the system to normal operations.*
1. Ensure that the fraudulent pages and/or email address are down.	
2. Keep monitoring the fraudulent URL.	*Sometimes a phishing website can reappear some hours later. In case a redirection is used and not taken down, monitor it very closely.*
3. At the end of a phishing campaign, remove the associated *Warning* page from the organizational website.	

PROCEDURE	PRINCIPLE
4. Verify all previous steps have been completed correctly.	
5. Return to the calling procedure and perform any remaining steps.	*Remaining steps may include, but are not limited to, close-out of other (parallel) steps such as privacy incident remediation, and incident documentation.*
2.1.19 PREPARING THE COMPUTER SECURITY INCIDENT REPORT (CSIR)	*The CMS/HHS Computer Security Incident Report (CSIR) template is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.*
2.1.19.1 PROCEDURE USERS	
1. On-site IR authority.	*Ideally, the CSIR should be filled-out by the on-site IR authority. Information should be gathered from all of the relevant sources, and documented in a coherent and consistent manner, preferably by someone with complete knowledge of all of the facts of the event.*
2. Business Owner.	
3. ISSO.	
4. SSO.	
2.1.19.2 ENTRY CONDITIONS	
1. A *Security Incident*, *Reportable Event*, or a data *Breach* is believed, or suspected, to have occurred.	
2. A previous procedure has directed that a CSIR be completed.	

PROCEDURE	PRINCIPLE
2.1.19.3 REPORT WRITING PROCEDURE	
1. Download the most recent CMS *Computer Security Incident Report (CSIR)* template from the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.	
2. Date and time:	
a. This is the data and time that the CSIR (report) was started.	
b. If the report is being updated; keep the original date on the report, but add *"Updated on mm/dd/20yy."*	*Some reports may be updated several times before they are closed.*
3. **Incident Tracking Number**:	*Located on the first table (on the cover page) of the CSIR template.*
a. If available, provide *the CMS Incident Number* assigned by the CMS CSIRT.	
b. If available, provide *the HHS Incident Number* assigned by the HHS CSIRC.	*If this number is available, the report author should be able to acquire this number from the CMS CSIRT.*
c. If available, provide *the CMS Incident Number* assigned by the US CERT.	*If this number is available, the report author should be able to acquire this number from the CMS CSIRT.*
4. **Reporting Individual Contact Information**:	*(Second table on the CSIR template.) This is the information of the CSIR AUTHOR. This individual should normally be the on-site IR authority that is the lead POC during the incident response process for **this** specific event.*
a. Name *(Required).*	
b. Email *(Required).*	
c. Office Number *(Required).*	

PROCEDURE	PRINCIPLE
d. Cell Number.	
e. Dept/OPDIV *(Required).*	
f. UserID.	
g. Name(s) of Dept/OPDIV or individual(s) notified of the security incident.	*This can be several individuals. It should include the CSIRT POC for this event, and may also include: the Business Owner, the applicable ISSO, CMS infrastructure support personnel (who may have provided technical support during the response phase), etc.*
5. **Impacted User Contact Information**:	*(Third table on the CSIR template.) This is the information on the person who INITIALLY REPORTED the incident.*
a. Name *(Required).*	
b. Email *(Required).*	
c. Office Number *(Required).*	
d. Cell Number.	
e. Dept/OPDIV *(Required).*	
f. UserID.	
6. **Incident Category**	
a. *Categorize* the incident in accordance with Figure 1.	*Categorize as CAT 1 through 6. Privacy incidents will hold a double categorization as CAT 1 through 6, AND is a PII/PHI incident.*
(1) For incidents involving a *Lost or Stolen Asset*:	
(a) Check the *Lost or Stolen Asset* checkbox.	
(b) Proceed to Step 9 and complete Section A, ***then return here for the next step.***	
(2) For incidents involving PII*:*	
(a) Check the *PII Breach* checkbox.	

PROCEDURE

(b) Proceed to Step 10 and complete Section B, ***then return here for the next step.***

(3) For incidents involving *Malicious Code*:

(a) Check the *Malicious Code* checkbox.

(b) Proceed to Step 11 and complete Section C, ***then return here for the next step.***

(4) For incidents involving *Unauthorized Access*:

(a) Check the *Unauthorized Access* checkbox.

(b) Proceed to Step 12 and complete Section D, ***then return here for the next step.***

(5) For incidents involving *Improper Usage/Policy Violation*:

(a) Check the *Improper Usage/ Policy Violation* checkbox.

(b) Proceed to Step 13 and complete Section E, ***then return here for the next step.***

(6) For incidents involving *Exercise/ Network Defense Testing*:

(a) Check the *Exercise/Network Defense Testing* checkbox.

(b) Proceed to Step 14 and complete Section F, ***then return here for the next step.***

PRINCIPLE

PROCEDURE	PRINCIPLE
(7) For incidents involving *Denial of Service, Scans/Probes/Attempted Access, & Investigations*:	
(a) Check the *Denial of Service, Scans/Probes/Attempted Access, & Investigations* checkbox.	
(b) Proceed to Step 15 and complete Section G, ***then return here for the next step.***	
b. Check the appropriate checkbox(s) for the *Type of Device Involved in the Incident*:	
(1) Blackberry.	*This includes ONLY CMS/HHS issued Blackberry devices. For all others, see PDA below.*
(2) Cell Phone.	*This includes any Government- or contractor-issued cell phones, or cellular access devices.*
(3) Computer (non-specific).	
(4) Computer Files.	
(5) Desktop Computer.	
(6) Domain Controller.	
(7) Email.	
(8) Hard-Drive (External).	
(9) Hard-Drive (Internal).	
(10) Laptop.	
(11) Paper Documents.	
(12) CD/DVD.	
(13) PDA.	*This includes ANY PDA or handheld remote connectivity device, either Government or contractor-issued, that can access email or other EXCHANGE-like services, or may have contained CMS sensitive data.*
(14) Server.	

PROCEDURE	PRINCIPLE
(15) Tape/DLT/DASD.	
(16) USB Thumb Drive.	
(17) Other.	
(18) Indicate the appropriate Operating System:	
(a) Windows.	
(b) Linux.	
(c) Unix.	
(d) Mac.	
(e) Other.	
c. Source IP/Network and/or Name.	*"Victim" machine.*
d. Destination IP/Network and/or Name.	*"Attacker" machine.*
e. Antivirus Vendor.	
f. Antivirus Signature Version Number.	
g. Indicate whether information was encrypted.	
(1) If yes, indicate Encryption Type/ Vendor.	
7. Verify that each of the applicable steps above have been completed to the maximum extent possible at this time.	
8. Return to the calling procedure.	*Return to the exact point in the procedure that instructed to complete the CSIR form. If the above procedure was followed verbatim, the applicable steps beyond this step should have already been completed.*
9. **Section A: Lost/Stolen Asset**	
a. Indicate if PII/PHI may have been exposed.	

PROCEDURE	PRINCIPLE
b. Provide a full description of the asset. Include the following: (1) Brand and model. (2) Location where the loss occurred. (3) Date and time the loss occurred. (4) Description of any information stored locally on the asset; and whether the local storage was encrypted. (5) All actions taken. (6) Return to Step 6.a. (1) (b)	
10. **Section B: PII Breach** a. Check the appropriate *Breach Category*: (1) Document Theft. (2) Hardware/Media Theft. (3) Document Loss. (4) Hardware/Media Loss. (5) Document Lost in Transit. (6) Hardware/Media Lost in Transit. (7) Improper Usage. (8) Unintended Manual Disclosure. (9) Unintended Electronic Disclosure. (10) Unauthorized Access. (11) Hacking or IT incident. (12) Document sent to Wrong Address.	
b. Indicate the *Number of PII Lost or Compromised*.	*Provide the number of individuals impacted by the incident. This will include the exact (or as near as possible) number of individuals whose data may have been compromised.*

PROCEDURE **PRINCIPLE**

c. Provide a description of the incident involving PII. Include the following:

(1) Brief description of the incident.

(2) Describe the roles of the people involved.

(3) Who the *Data Owner* is of the PII.

(4) The type of PII involved.

(5) The number of individuals impacted.

(6) The current status of the affected data.

(7) Remedial action taken to date.

(8) Planned future remediation actions.

d. Return to Step 6.a. (2) (b)

11. **Section C: Malicious Code**

a. Check the appropriate checkbox(s) for the *Malware Type*:

(1) Worm.

(2) Virus.

(3) Trojan.

(4) Buffer Overflow.

(5) Denial of Service.

(6) Other.

b. Check the appropriate checkbox(s) for the *Operating System*:

(1) Windows.

(2) Linux.

(3) Unix.

(4) Mac.

PROCEDURE **PRINCIPLE**

(5) Other.

c. If known, provide the malware *Name.*

d. Check the appropriate checkbox for the *Action Taken Regarding the Malware*.

(1) Quarantined.

(2) Cleaned.

(3) Left Alone.

e. Check the appropriate checkbox for whether, *prior to the event*, the affected node was properly patched.

f. Provide a description, including timelines, of all of the actions taken and all planned actions.

g. Return to Step 6.a. (3) (b)

12. **Section D: Unauthorized Access**

a. Provide a description, including timelines, persons involved, and data accessed, associated with the *unauthorized access*.

b. Provide a description, including timelines, of all of the actions taken and all planned actions.

c. Return to Step 6.a. (4) (b)

13. **Section E: Improper Usage/Policy Violation**

a. Check the appropriate checkbox(s) for the *Type of Violation*.

(1) (P2P) File Sharing.

(2) Instant Messenger.

(3) Inappropriate Web Sites.

(4) Remote Access.

(5) Unapproved Software.

PROCEDURE **PRINCIPLE**

(6) Other.

(a) If applicable, describe in a short sentence.

b. Provide a description, including timelines, persons involved, and data accessed, of the violation.

c. Provide a description, including timelines, of all of the actions taken and all planned actions.

d. Return to Step 6.a. (5) (b)

14. **Section F: Exercise/Network Defense Testing**

a. Provide the Name of the person who provided approval for the testing.

b. Provide a 10-digit contact number for the person who provided approval for the testing.

c. Provide a reason and description, including timelines, of all of the testing.

d. Return to Step 6.a. (6) (b)

15. **Section G: Denial of Service, Scans/ Probes/Attempted Access, & Investigations**

a. Provide a description, including timelines, hardware, software, and persons involved of the violation.

b. Provide a description, including timelines, of all of the actions taken and all planned actions.

c. Return to Step 6.a. (7) (b)

2.2 TABLES AND FIGURES

Table 1 Breach Assessment Guidelines

Category	Examples	Rationale	Action
Hard copy documents containing PII/ PHI go to wrong provider.	CMS business associate (e.g., MAC, FI, Carrier, other Medicare contractor) sends remittance advice to wrong provider. Data elements may include full HICN, beneficiary name, address, DOB, procedure codes, claims info.	Reliance on provider being subject to privacy and security requirements under HIPAA and/or State law. Providers are obligated to protect the privacy and security of PII/PHI received in the same or similar manner as the CMS business associate that disclosed the information.	CSIRT documents that the incident falls within the guideline (and includes in monthly report to the HHS CSIRC) and also coordinates operational mitigation activities/ corrective action with business associate as appropriate; outreach and education instructs providers to destroy PII/PHI and alert contractors to mismailing.
Hard copy documents containing PII/ PHI go to wrong beneficiary.	CMS business associate (e.g., MAC, FI, Carrier, other Medicare contractor) sends Medicare Summary Notice to wrong beneficiary. Data elements may include last four digits of HICN, beneficiary name, address, DOB, procedure codes, claims info.	Low likelihood of significant financial, reputational, or other harm to affected beneficiary: 1. Beneficiary reported mismailing to business associate, PII/PHI not intentionally accessed, very little likelihood beneficiary knew the other. 2. Low risk of financial harm resulting in ID theft given data elements contained in MSN (not complete SSN/HICN). 3. Procedure code may be included but not diagnostic info.	CSIRT documents that the incident falls within the guideline (and includes in monthly report to the HHS CSIRC) and coordinates operational mitigation activities/corrective action with business associate as appropriate (e.g., messaging on MSN); outreach/ education to business associates.

Figure 1 Incident Categories

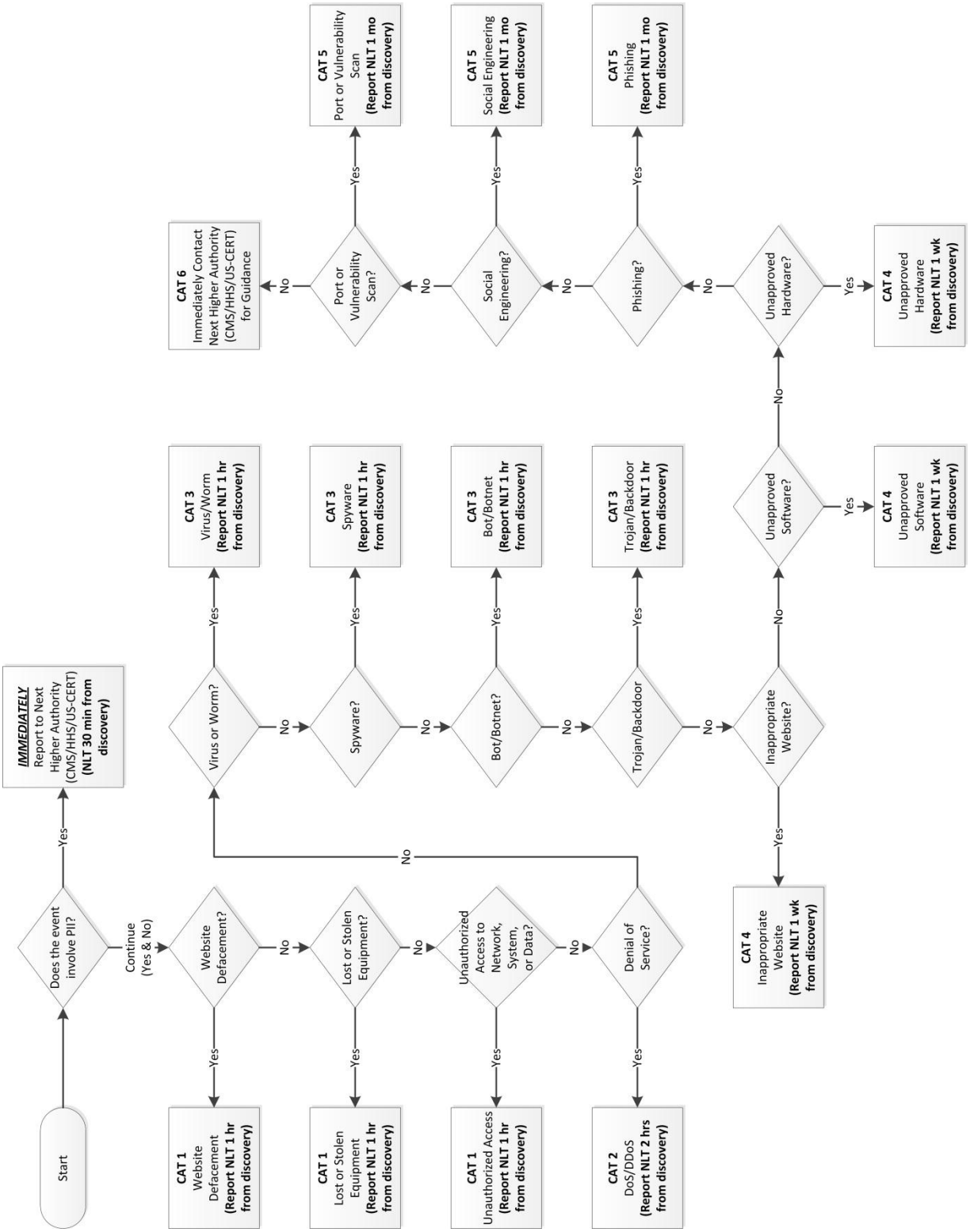
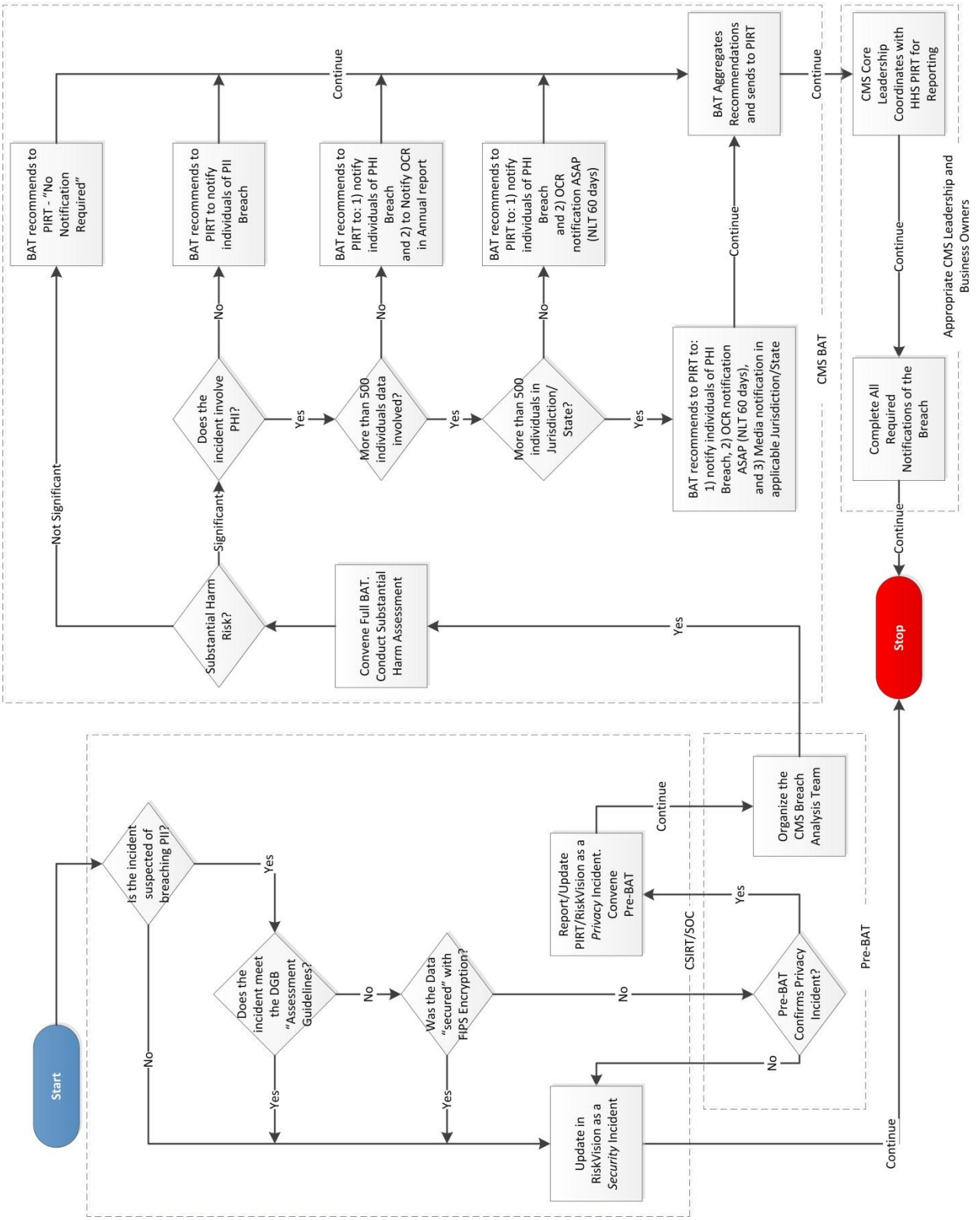


Figure 2 Breach Assessment and Notification Process



3 APPROVED

teresa.fryer@cms.hhs.gov

Digitally signed by teresa.fryer@cms.hhs.gov
DN: cn=teresa.fryer@cms.hhs.gov
Date: 2012.12.12 15:11:57 -05'00'

Teresa Fryer
CMS Chief Information Security Officer and
Director, Enterprise Information Security Group

This document will be reviewed periodically, but no less than annually, by the Enterprise Information Security Group (EISG), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the EISG at mailto:ciso@cms.hhs.gov.