Technical “Large” Cyber Incident Handling Steps

1. Purpose
   The Best Practices workgroup was tasked to provide national industry standard best practices for Incident Response and Incident Handling of large cyber related incidents. This document is to provide technical best practices on dealing with a high or critical cyber incident.
2. Policy
   Large Cyber Incident Handling applies to the following controls found within the Information Security Policy.
   a. Information Security Policy
      - Respond
        - 4.1.2, 4.1.3, 4.4, 4.5, 4.6, 4.7.2

   b. Information Security Policy – Appendix A
      - Incident Response (IR)
        - IR-1
        - IR-4
        - IR-5
        - IR-6
        - IR-7

3. Large Cyber Incident Response Steps

Examples of what can be considered a large incident:

- Malicious code or computer virus incident that affects a large group of people (agency size dictates the definition of Large – greater than 25%)
- Natural disaster that affects computer systems
- Unscheduled power outage with a break in services
- Unscheduled enterprise network outage
- Enterprise hacking attempt including alteration of static web site content
- Physical infrastructure sabotage or failure
- System compromise
- Cyber terrorism
- Denial of Service (DoS) attack
- Keylogger incident
- Loss or alteration of data including confidential and sensitive data
- Loss or alteration involving federal tax information, protected health information, PII, or personal financial information, Critical Infrastructure, Military, Law Enforcement, or University Information.

Preparation Phase:

1. Each organization shall develop and document an Information Systems Incident Response (ISIRT) team and be prepared to handle incidents.
2. Organizations shall use the ISIRT template provided as a model in developing an incident handling plan within their organization.

Detection & Analysis Phase:

NOTE Refer to the ISIRT manual for detailed information.

1. Actions performed on the information system should cease, or be kept to a minimum if possible in order to preserve the integrity of evidence.

2. Once confirmed the incident is real the organizations Information Systems Incident Response Team (ISIRT) should be activated by authorized management.

3. The Incident Commander (IC) of the organizations ISIRT must call the SITSD Network Operations Security Center (NOSC) (444-2000) within 24 hours of incident. The IC will document the time when this occurs. The NOSC will create a service ticket and direct the IC to the Incident Report Form (agency shall fill out the Form). Once the NOSC ticket is created, the NOSC will sent out communication to the Security Threat Group alerting them that an

Incident Report is being filled out and to soon expect the report from the agency. The agency will send the filled out Incident Report Form via secure communications to the ISSO office, and the ISSO office will share with the rest of the Security Threat Group via secure communications. The Security Threat Group is made up of reporting agency, SITSD-Information Systems Security Office (ISSO), Montana All-Threat Intelligence Center (MATIC) and Department of Military Affairs. See Security Incident Flowchart.

4. Review of SIEM data, packet captures (PCAP), automated detection logs, 3rd party information, IDS/IPS logs, etc. should be performed verifying validity and scope of the incident.

5. The IC will continue documenting important events, with timestamps, as they unfold until a delegated authority is assigned to take over this duty.

6. Notification to

    a. Risk Management and Tort Defense Division (RMTD) will be made immediately (444-2421). RMTD Report form must also be completed and submitted to them. Information gathered from the Incident Report Form can be used to fill out RMTD Report form.
    b. If incident involves sensitive data immediately report loss or theft to appropriate law enforcement agencies.
    c. If incident involves Federal Tax Information (FTI) a notification to the Office of Safeguards no later than 24 hours after identification of possible issue involving FTI. Call the Denver TIGTA Field Division at 303-291-6100 or National Office Hotline for TIGTA 800-589-3718. **Call the Denver TIGTA Filed Division Office first.**
    d. If a breach of unsecured protected health information, a covered entity must notify the Secretary of HHS of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. The covered entity must submit the notice electronically by submitting the form found at the following site: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf. Alternatively, if the Office of Civil Rights (OCR) can be called at 1-800-368-1019.
    e. *SSA Required Language:* If your agency experiences or suspects a breach or loss of PII or a security incident which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement (currently Lynne Pizzini). That State official or delegate must then notify the SSA Regional Office Contact (Tracy Tweten tracy.tweten@ssa.gov (303)844-0839 alternate email den.cps@ssa.gov) or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact **within one hour**, the responsible State Agency official or delegate must report the incident by contacting **SSA's National Network Service Center (NNSC) toll free at 877-697-4889** (select "Security and PII Reporting" from the options list). The EIEP will provide updates as

they come available to SSA contact as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.

f. If an incident involves data that may be protected under the Family Educational Rights and Privacy Act (FERPA), consider notifying Family Policy Compliance Office (FPCO) about the breach. (FERPA does not require that you notify FPCO of the breach; however, the U.S. Department of Education considers it a best practice. While FPCO has the discretion under 34 CFR §99.64(b) to conduct its own investigation of a breach, it will take into consideration an effort to proactively come into compliance demonstrated by voluntarily notifying FPCO about the breach.) The number to contact FPCO is 1-800-47-8733 (which is the Office of Inspector General Fraud Prevention involving the U.S. Department of Education).

7. The Incident Report should be completed as soon as possible.

Containment Phase:

8. If the system is a physical device and is running destructive software (formatting, deleting, removing or wiping information), power to the system should be disconnected immediately to preserve evidence that is left on the machine if possible (pulling the plug). A similar action should be performed on virtual machines by performing a "Power Off" action. If the system is not running destructive software do not pull the power.

9. If the incident has the potential for damage and/or theft of resources such as sensitive data, then a quick **netstat -a -o -b** (on Microsoft Windows**)** using the cmd command line tool with administrative privileges should be run and results saved. (If using Linux the command is **netstat -anp**) If the information system is a virtual machine, then a complete snapshot, including memory, will be taken. Internet connectivity on the system(s) will be disabled after performing these steps.

10. If the organization has sandboxing capabilities and it is determined that there is acceptable risk with no legal ramifications to gather threat intelligence, then immediate redirection to the sandboxed environment will be done. This could be in the form of strict network segmentation not allowing specific subnets to communicate with each other. This is in order to gather information to determine if, or what, other systems may be involved.

11. If the system is communicating with any IP addresses and domain names for known Command and Control (C2) channels, those IP addresses and domain names should be blocked at the perimeter.

12. If determined forensic investigation of an information system is needed (determined by agency ISIRT), any further interactions with the information system(s) by IT staff should immediately stop. System administrators must take into account that access to a physical device through

either a USB or, if possible, a network connection must be available to the forensic investigators.

13. A Chain of Custody will be established by a Digital Forensics Analyst if there is any possibility of a legal investigation. Limiting physical access to the information system is a must in order to preserve the integrity of the Chain of Custody.

14. Forensic analysis by a Digital Forensic team, or 3rd party forensic company, will begin. An attempt to perform triage forensics will be prioritized in order to provide system administrators and upper level management with critical information that may help with the containment and/or eradication phases. Management must understand that full forensic analysis of system(s) could take a long time.

Eradication Phase:

15. After containment, eradication should be performed to eliminate components of the incident. Identifying all affected hosts within the organization is critical so they can be remediated. Some incidents may not require harsh eradication techniques and actions taken should be approved by upper level management.

16. Actions such as deleting malware, disabling breached user accounts, identifying and mitigating vulnerabilities, or complete rebuild of the information systems should be performed if approved by management.

17. Deactivation of the organizations ISIRT can be performed at this time. Documentation created during the ISIRT will be collected for use in the post-incident report.

Recovery Phase:

18. Once the incident on information system(s) have been eradicated returning affected systems to normal operation can begin. This may involve actions such as restoring from clean backups, rebuilding systems, installing patches, changing passwords, and tightening network security.

19. Higher level of system logging and/or network monitoring should be considered on all systems within an organization due to the increased chance of system(s) being attacked again.

20. Confirmation systems are functioning normally and vulnerabilities are remediated should be performed to prevent similar incidents.

Post-Incident Activity:

21. Documentation created during the incident should be used to prepare a post incident report. This report should include items such as cause, Plan of Actions and Milestones (POA&M) or Gap analysis, lessons learned, cost, need for evidence retention, recommendations for immediate action, and long term goals to prevent another similar incident.

22. Information sharing to the Security Threat Group and other organizations should be considered to help prevent similar incidents to others.

See next page for Incident Handling Checklist

Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

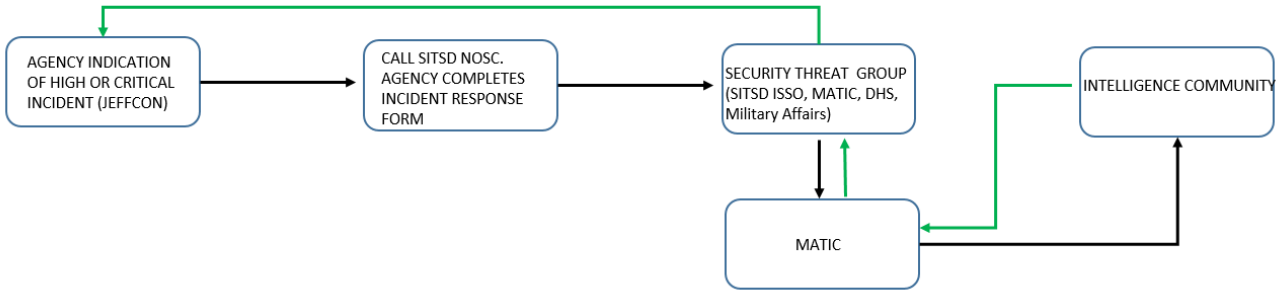
Cichonski, Paul. Millar, Tom. Grance, Tim. Scarfone, Karen. “Computer Incident Handling Guide” *National Institute of Standards and Technology*. NIST, August 2012, Web. 1 April 2016

Dissemination of Security Incident Form

Initiation of Security Incident Form:

1. Large Cyber Incident Response is initiated when an organization, department, or agency discovers or is notified or a large incident (a high or critical incident based on the JeffCon scale).
2. The Incident Response Form is filled out when reaching Step 3 in the Large Incident Response Steps; contacting the SITSD NOSC (444-2000).

Security Incident Flowchart:



Dissemination of Security Incident Form:

1. After completing the Security Incident Form, the agency securely sends the form to the ISSO, the ISSO will securely send the form to the rest of the Security Threat Group.

2. The Security Threat Group conducts analysis on the incident and distributes form and analysis to the MATIC as well as relevant affected agencies if warranted.

3. The MATIC passes raw information to the Intelligence Community (DHS, FBI, CYBERCOM…)

4. If possible, the Intelligence Community conducts analysis and sends feedback to the MATIC.

5. The MATIC passes feedback to the Security Threat Group.

6. The Security Threat Group distributes findings and feedback to the originating agency.

Information Security Incident Report Form:

Click here for latest form.

STATE OF MONTANA INFORMATION SECURITY INCIDENT REPORT FORM

State Agency:	
Security Contact Information:	
Incident Reported By:	

Incident Title:	
Incident Number:	
Report Date:	
Date & Time of Incident:	
Date & Time Resolved:	

Statement of Incident: (Describe the type of Incident, how incident was discovered, level of unauthorized access attained, what did the event accomplish, the impact to your services (offline, length of time), did the incident affect any sensitive data (PII, FTI, HIPPA), what is the current system status)
Impact of the Incident/Systems Affected: IP Address(es) Hostname(s) Purpose of System(s) Operating System & Version Ports of Communication Utilized Physical Location Attack Vector Utilized / Exploited Evidence discovered Additional Details
Technical Details:
Immediate Actions:
Steps Taken to Prevent Recurrence:

Description of Attachments (if applicable, such as logs, reports or screenshots):	

Changes since Version 06-08-2016

Page 9 – Moved "Initiation of Security Incident Form:" section above the flowchart diagram to help with definition of high or critical while viewing flowchart (Lance Wetzel MDT recommendation)

Page 5 Step 9 – Added Linux command to this step (Stewart Fuller HHS recommendation)

Changes since Version 06-30-2016

Page 3 & 4 Step 3 – Changed name of Service Desk to NOSC. Added Department of Military Affairs to Security Threat Group.

Page 9 – Changed name of Service Desk to NOSC.

Page 9 – Updated flowchart to reflect NOSC and Military Affairs.