This document describes the Incident response procedures for security incidents that occur in the secure research project repository.

Roles and Responsibilities of key stakeholders:

a) ISPO/Research Data Security Specialist (RDSS)
    - responsible for coordinating the FSU Incident Response.
    - Identifies and preserves any appropriate log data which may be used in the investigation process.
b) ISPO Operation Team staff
    - Provide any support necessary to the ISPO/Research Compliance Coordinator.
c) ITS MEAS/LEAS/CTS/NCT System Administrators
    - responsible for investigating the incident and reporting findings at the direction of the ISPO/Research Compliance Coordinator.
    - responsible for collecting evidence by taking snapshots and clones of systems under their management.
    - Will gather log data as requested.
d) Research Principal Investigators (PI) and other staff (researchers) who utilize Controlled Unclassified Information
    - The primary users of the data will need to be trained on these procedures and notify appropriate parties upon identification of any suspected cyber incidents relating to this information.

Overview:

Incident Response Procedures:

The Florida State University Information Security and Privacy Office has developed Incident Response Procedures. This document follows these procedures whenever possible.

Incident Response Training:

As required by the relevant NIST SP 800-53 Security Control IR-2 Incident Response Training, and by the NIST 800-171 controls 3.6.1 “Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities” and 3.6.2 “Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization”. FSU will provide Incident Response Training to information system users consistent with assigned roles and responsibilities within [as yet to be determined time period] of assuming an incident response role or responsibility, when required by information system changes and [at a to be determined frequency] thereafter.

FSU policies and procedures do not currently specify a timeframe or frequency for providing Incident Response training. These timeframes will need to be defined.

Incident Response Testing:

As required by the relevant NIST SP 800-53 Security Control IR-3 Incident Response Testing and by the NIST 800-171 control 3.6.3 “Test the organizational incident response capability”. FSU will test the incident response capability for the information system [at a to be determined frequency] using [as yet to be determined organization-defined tests] to determine the incident response effectiveness and documents the results.

FSU policies and procedures do not currently specify a frequency for providing Incident Response testing. This timeframe will need to be defined. FSU policy and procedures do not currently define any tests required when testing Incident Response procedures. These tests will also need to be defined.

As required by the relevant NIST SP 800-53 Security Control IR-3(2) Incident Response Testing, Coordination with Related Plans and by the NIST 800-171 control 3.6.3 “Test the organizational incident response capability”. FSU will coordinate the incident response testing with organizational elements responsible for related plans. This includes for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

FSU does not currently have detailed testing plans regarding Controlled Unclassified Information. These plans will need to be developed in conjunction with any currently existing Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

Incident Handling:

As required by the relevant NIST SP 800-53 Security Control IR-4 Incident Handling and by the NIST 800-171 controls 3.6.1 “Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities” and 3.6.2 “Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization”. FSU has developed an Incident Response Procedure that must be followed in the event of a cyber security incident impacting Controlled Unclassified Information. These procedures are to be followed.

Incident Monitoring:

As required by the relevant NIST SP 800-53 Security Control IR-5 Incident Monitoring and by the NIST 800-171 controls 3.6.1 “Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities” and 3.6.2 “Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization”. FSU has developed an Incident Response Procedure that includes the tracking and documentation of information system security incidents by the Director of the Information Security and Privacy Office. These procedures are to be followed.

Incident Reporting:

As required by the relevant NIST SP 800-53 Security Control IR-6 Incident Reporting and by the NIST 800-171 controls 3.6.1 “Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities” and 3.6.2 “Track, document, and report incidents to designated officials and/or authorities both internal and

external to the organization". FSU has developed an Incident Response Procedure that includes the requirement for immediate reporting of information system security incidents to the Director of the Information Security and Privacy Office. These procedures are to be followed. Additionally, if the grant or contract covering Controlled Unclassified Information specifies additional Incident Reporting, these procedures are to be followed as well.

Incident Response Assistance:

As required by the relevant NIST SP 800-53 Security Control IR-7 Incident Response Assistance and by the NIST 800-171 controls 3.6.1 "Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities" and 3.6.2 "Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization". FSU has developed an Incident Response Procedure that includes provisions for an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The FSU Incident Response Procedures are to be followed.

Incident Response Procedures:

Within 72 hours of the discovery of a cyber incident:

- Investigate the cyber incident. When a cyber incident is discovered that affects a covered contractor's information system, covered defense information or a contractor's ability to provide operationally critical support, conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This includes analyzing covered contractor information system(s) that were part of the cyber incident, as well and other information systems on the contractor's network(s) that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the contractor's ability to provide operationally critical support. (Source: DFARS 252.204-7012(c)(1)(i).)
- Identify, isolate and be prepared to provide a copy of any malicious software as may be requested by the DC3 or contracting officer. (Source: DFARS 252.204-7012(d).)
- Preserve and protect images of all known affected information systems and all relevant monitoring/packet data for at least 90 days from submission of the cyberincident report to allow the DOD to request the media or decline interest. (Source: DFARS 252.204-7012(e).). (Take and retain snapshots or clone images of any systems before making any changes to them as part of any remediation efforts whenever possible).
- If FSU is the prime contractor (or acting as both the prime and sub-contractor). Within 72 hours of discovering the cyber incident:
    - Rapidly report a DFARS cyber incident by filling out and submitting an Incident Collection Format (ICF) via the DIBNet portal (http://dibnet.dod.mil). On the main page, there is a link to the ICF for Defense Industrial Base (DIB) reporting. (Source: DFARS 252.204-7012(c)(1)(ii).)

    - If you do not have all the information required by the clause report what is available. As more information becomes available, provide updates to the Defense Cyber Crime Center (DC3).
    - Upon receipt of the contractor submitted ICF in the DIBNet portal, the DC3 will send an unclassified e-mail containing the submitted ICF to the contracting officer identified on the ICF. DC3 is the designated collection point for cyber incident reporting required under DFARS Clause 252.204-7012.
- If FSU is a subcontractor:
    - Report the incident to the prime contractor. The prime contractor will then submit an incident to the DC3. (I have found conflicting information on this. To be prudent, FSU should probably submit this to the DIBNet portal (http://dibnet.dod.mil) as well).
- Provide access upon request by the DOD to additional information or equipment necessary to conduct a forensic analysis. (Source: DFARS 252.204-7012(f).)
- If the DOD elects to conduct a damages assessment, provide all of the damage assessment information gathered in connection with the media preservation and protection provisions of DFARS 252.204-7012(e). (Source: DFARS 252.204-7012(g).)
- When providing information, to the maximum extent practicable, identify and mark attributional/proprietary information to allow the DOD to safeguard the contractor's attributional and proprietary information. This is important because any information obtained under this clause may be used and released outside of the DOD for purposes and activities authorized by DFARS 252.204-7012(i) and "for any other lawful Government purpose or activity" subject to restrictions on the government's use and release of such information under DFARS 252.204-7012(j). (Source: DFARS 252.204-7012(h).)
- Conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use and disclosure of electronic communications and data. (Source: DFARS 252.204-7012(k).)

Detailed Procedures:

Upon discovery of a suspected security incident:

If the PI or a researcher discovers the suspected incident: The PI/researcher should open an FSU Service Center CRM case. The Specialty Type for this case will be NIST. Please provide as much information as possible. The case will be routed to the NIST support team who will triage the case and route it appropriately.

If the suspected incident is discovered by the ITS staff, ISPO staff or the RDSS, then they should open a CRM ticket for tracking purposes. The Specialty Type for this case will be NIST.

Once the NIST team receives the ticket, after reviewing it and confirming that there is evidence to suspect that a suspicious security incident has occurred, they should send an email to the ISPO Operations Team (ISPO-SOC-Team@fsu.onmicrosoft.com) with details of the suspected incident. They

should then begin the process of evidence gathering including gathering copies of malicious software, images of affected systems, packet data & log data.

The ISPO Operations team should then contact the RDSS and start the incident resolution process (https://security.fsu.edu/sites/g/files/upcbnu581/files/FSU%20Incident%20Response%20and%20Reporting%20Procedures%20August%202015.pdf). The RDSS will contact the appropriate federal entities or primary contactor as appropriate for further response guidance and forensics recommendations. The RDSS will be the primary interface between the federal responders and FSU.

After hours on call support is available for suspected security incidents. The originator should call the on call number at (850-644-HELP) and inform the operator that this is a NIST issue and it should be escalated to the on call MEAS team. The MEAS team member will then review the issue and after confirming that there is evidence to suspect that a suspicious security incident has occurred, they should email (ISPO-SOC-Team@fsu.onmicrosoft.com) then call (850-645-ISPO) the ISPO Operations Team with details of the suspected incident.

FSU Research Project Security Incident Response process diagram

NIST 800-171 Compliance