WARNING – Internal Use Only

Guidance Document – DFARS 252.204-7012 Cyber Incident Reporting

Applies to Classification level: Controlled Unclassified Information

Contents

Purpose

In order to establish a documented and uniform process whereby project personnel engaged in research with specific Cyber incident reporting requirements understand their Cyber incident reporting requirements and roles as outlined in *DFARS 252.204-7012*. This process is meant to minimize unnecessary communications, decrease time to resolution, and ensure reporting requirements are met.

Roles & Responsibilities Cyber Incident

Name	Role	Actions
	Primary Incident Arranger	Communication, Reporting Coordination, Submits the data provided by the Incident Responder to DIBNet. Cyber Incident Damage Assessment Activities
	Backup Incident Arranger	Communication, Reporting Coordination, Submits the data provided by the Incident Responder to DIBNet. Cyber Incident Damage Assessment Activities
	Primary Incident Investigator Manager	Manager for Forensic Analysis, Media Preservation and Protection
	Backup Incident Investigator	Forensic Analysis, Media Preservation and Protection
	Security Engineer	Consultation for audits and alert ingest to the SEIM
	Security Architect	Consultation for Security Architecture
	Cyberinfrastructure	Consultation for Research Architecture

	Architect	
	System Engineer	Primary contact to provide the incident investigator ability to the perform forensic analysis and media preservation, local system Audit and Alert
	Program Manager	Provides staff coordination and communication with research and Export Controls and Research Information Assurance
	Information Assurance	Executive Sponsorship and Manager Export Control and Research Information Assurance.
	Regulatory Analyst	Determine if your institution is required to report any of its activities in accordance with Department of Commerce regulations (15 CFR Part 781 et seq.) or Nuclear Regulatory Commission regulations (10 CFR Part 75) Help to determined scope of the project, contract terms and staff assigned

Scope for Research Data

Research data either subject to publication restrictions or dissemination controls or which involves proprietary or controlled inputs that make it subject to regulations. Controlled Research is often protected with a Technology Control Plan.

Terms:

Controlled technical information **-** means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Contractor attributional/proprietary information **-** means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

Covered defense information **-** means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or

dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Technical information **-** means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Scope for Information System and Instruments

Information System - means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information within scope of Controlled technical information, Contractor attributional/proprietary information, Covered defense information, and Technical information.

Terms:

Cluster – means a discrete set of research systems (Front Ends, Backends, Storage) created a research cluster for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information within scope of Controlled technical information, Contractor attributional/proprietary information, Covered defense information, and Technical information.

- Hardware - means compute nodes + interconnect + storage
- Software – means OS + compilers + libraries + apps + queue manager
- Infrastructure – means front-ends + power + cooling + data center + staff
- *Approved File-Storage* - means a system to archive and or temporally store data within EC/IAO approved storage locations and listed in a TCP or SSP
- *Front-end:* means accepts requests and routes them to a backend node.
- *ThinLic* - means a Linux remote desktop server. It is the component which enables remote access to Weber, resuming disconnected sessions and load balancing of sessions
- *Backend Servers (nodes)* - means research systems used to access, store, produce and/or process information within the weber cluster hosted within the trusted network.
- Job - means simply a set of tasks to be performed by a cluster. Cluster executes jobs on back-end compute nodes
- Queue – means Jobs are submitted to a queue, with constraints on jobs based on max nodes, and walltime, and priorities.
- *Audit Server* - means systems used to capture log data from <add your systems>

- *Backup system -*

Desktops - means systems used to access, store, produce and/or manipulate other assets, authorized systems are recorded in a Technology Control Plan, all other systems would be considered unauthorized.

Laptops - means systems used to access, store, produce and/or manipulate other assets, authorized systems are recorded in a Technology Control Plan, all other systems would be considered unauthorized.

Mobile devices - means systems used to access other Assets (tablets, smartphones, smartwatches)

Sensors - means a discrete set of research with sensor instruments (e.g., network-connected neutrino collectors)

Network-connected scientific control systems – means a discrete type of research equipment with specific functions, (e.g. microscopes, telescopes, light sources, particle accelerators)

Diagram Cluster:

<add diagram>

User Data Ingress Diagram:

<add diagram>

User Data Egress Diagram:

<add diagram>

What is a Cyber Incident?

Report cyber incidents Within 72 hours of discovery of any cyber incident to DoD at http://dibnet.dod.mil.

Terms:

Cyber Incident **-** means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Compromise **-** means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

WARNING – Internal Use Only

Malicious software **-** means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

Adequate Security - means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information. **Requires a Technology Control Plan or System Security Plan.**

In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents.

The following staff have access to a medium assurance certificate:

- <Primary Incident Arranger>
- <Backup Incident Arranger>

Reporting an Incident:

- A list of approved information systems and personal listed on a Technology Control Plan or System Security Plan can be obtained from"
    - <storage location>

Reported to Regulatory Analyst and Information Assurance:

- Determined is in scope of DFARS 252.204-7012, if yes:
    - Incident Investigator submits an incident to <regulatory office contact>
    - Incident Investigator procedure to determines if there has been a:
        - actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein
        - disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.
        - computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

- Regulatory Analyst Determines If the Contractor is required to report any of its activities in accordance with Department of Commerce regulations (15 CFR Part 781 et seq.) or Nuclear Regulatory Commission regulations (10 CFR Part 75) in order to implement the declarations required by the U.S.-International Atomic Energy Agency Additional Protocol (U.S.-IAEA AP).
- See Incident Investigator Incident Response Procedures for more details.

Reported to Security Office:

- Determined is in scope of DFARS 252.204-7012, if yes:
  - Incident Investigator submits an incident to <regulatory office contact>
  - Investigator begins procedure to determines if there has been a:
    - actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein
    - disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.
    - computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.
  - Regulatory Analyst Determines If the Contractor is required to report any of its activities in accordance with Department of Commerce regulations (15 CFR Part 781 et seq.) or Nuclear Regulatory Commission regulations (10 CFR Part 75) in order to implement the declarations required by the U.S.-International Atomic Energy Agency Additional Protocol (U.S.-IAEA AP).
  - See Incident Investigator Incident Response Procedures for more details.

Discovered by Security Analyst:

- Determined is in scope of DFARS 252.204-7012, if yes:
  - Submit incident to <your incident reporting contact or create a internal incident>
  - Incident Investigator submits an incident to <regulatory office contact>
  - Investigator begins procedure to determines if there has been a:
    - actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein
    - disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or

unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

- computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

- Regulatory Analyst Determines If the Contractor is required to report any of its activities in accordance with Department of Commerce regulations (15 CFR Part 781 et seq.) or Nuclear Regulatory Commission regulations (10 CFR Part 75) in order to implement the declarations required by the U.S.-International Atomic Energy Agency Additional Protocol (U.S.-IAEA AP).
- See Incident Investigator Incident Response Procedures for more details.

Regulator Office:
Will determine if the Contractor is required to report any of its activities in accordance with Department of Commerce regulations (15 CFR Part 781 et seq.) or Nuclear Regulatory Commission regulations (10 CFR Part 75) in order to implement the declarations required by the U.S.-International Atomic Energy Agency Additional Protocol (U.S.-IAEA AP).

Incident Investigator:

Terms:
Media **-** means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

Forensic Analysis **-** means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Operationally critical support **-** means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

1. When the institution> discovers a cyber incident within scope of *DFARS 252.204-7012* has occurred, the institution> must conduct a review for evidence of compromise of covered defense information
2. As the Incident Responder, you analyze the covered contractor information system(s) that were part of the cyber incident, as well as 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.

3. The Incident Coordinator must report the incident within 72 hours of discovery to DoD. The Incident Coordinator will need at least 1.5 hours to review the report and create the incident. The media will not be uploaded to the DoD site at this time. DoD to request the media or decline interest.

Note: In most occurrences, the institution will not be providing critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation, thus we should not have information systems that provide operationally critical support.

Media preservation and protection:

The institution shall preserve and protect images of

- Identified user accounts. (e.g legal holds, exports, identifiers)
- All known affected information systems (e.g. compromised computers, servers, specific data)
- Monitoring/packet capture data
- Keep the data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.
- Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis. Do not send the malicious software to the Contracting Officer.

Malicious Software Submission:

If the Incident Investigation discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

- https://www.dc3.mil/ (core site)
- https://www.dc3.mil/digital-forensics#submit-a-case
    - Intrusions Laboratory Request Form.
        - Example here: link
        - Customers will also ensure classification markings of individual items and overall collections are quickly and readily identifiable.
        - Media Classification Level will be determined at the time of incident, options below.

WARNING – Internal Use Only

UNCLASSIFIED
FOR OFFICIAL USE ONLY
CONFIDENTIAL
SECRET
S//NOFORN
TOP SECRET
TS//NOFORN
TS//SCI

The following items must be included (where applicable) with submitted evidence for DC3/CFL to perform an examination:

• Completed and signed DC3/CFL Form 1A - Intrusions Laboratory Request
• Search authority documentation
• Evidence listing
• Chain of custody document(s)
• Customer reference numbers for evidence, as required by customer regulations
• Witness statements and/or discussions
• Subject statements
• Copy of charge sheet(s)
• Reports/Notes detailing any prior analysis conducted by someone outside DC3/CFL to include online investigations
• Notes on DC3/CFL Form 1A regarding media that has been damaged prior to shipment to DC3/CFL
• Notes on DC3/CFL Form 1A indicating which person each piece of evidence is associated with, if known (e.g. subject's
thumb drive, victim's laptop, etc.)
• Passwords to files/devices (e.g. from a Post-It note of passwords located near the device at a crime scene or ones provided
by subjects during interviews)
• Any other related equipment or information that would increase probability of full access to case-relevant data

Incident Arranger:

Submitting an incident:

Determine if there is malicious software, if yes do we need to submit to DoD Cyber Crime Center (DC3)?

- The institution shall report as much of the following information as can be obtained to DoD within 72 hours of discovery of any cyber incident to DoD at https://dibnet.dod.mil/portal/intranet/.
- Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

Question	Answer, Action, or Contact
Company name	
Company point of contact information (address, position, telephone, email)	
Data Universal Numbering System (DUNS) Number	
Contract number(s) or other type of agreement affected or potentially affected	
Contracting Officer or other type of agreement point of contact (address, position, telephone, email)	
USG Program Manager point of contact (address, position, telephone, email)	
Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)	
Facility CAGE code	
Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)	
Impact to Covered Defense Information	
Ability to provide operationally critical support	
Date incident discovered	
Location(s) of compromise	
Incident location CAGE code	
DoD programs, platforms or systems involved	

Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)	
Description of technique or method used in cyber incident	
Incident outcome (successful compromise, failed attempt, unknown)	
Incident/Compromise narrative	
Any additional information	

Note: The Government shall protect against the unauthorized use or release of information obtained from the institution to the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released. See DFARS 252.204-7012 for more details.

If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in initial investigation.