<?xml encoding="UTF-8">

5352.204-9002 Security Incident Reporting and Procedures

As prescribed in DAFFARS 5304.404-90 Additional Contract Clauses, insert the following clause in solicitations and contracts:

SECURITY INCIDENT REPORTING AND PROCEDURES (JUN 2024)

(a) The contractor shall follow the below guidance when a contract contains a DD Form 254, DOD Contract Security Classification Specification:

(1) The contractor shall notify the Government Contracting Activity (GCA) of any security incident involving the potential or actual loss, compromise, or suspected compromise of Top Secret, Secret, and/or Confidential information, referred to as classified information, when the incident is discovered at the contractor's location.

(i) The contractor shall conduct the requisite inquiry(ies) in accordance with 32 CFR Part 117 and Cognizant Security Office (e.g., Defense Counterintelligence and Security Agency) guidance.

(2) Security incidents occurring at government performance locations where the contractor is categorized as a visitor will be processed and reported in accordance with government host security procedures.

(3) Security incidents involving the potential or actual loss, compromise, or suspected compromise of Special Access Program and/or Sensitive Compartmented Information is under the jurisdiction of the GCA and the contractor shall follow GCA guidance in lieu of this requirement.

(4) This requirement does not relieve the contractor from reporting requirements set forth in 32 CFR Part 117, DFARS 252.204-7012, or as otherwise directed by contract requirements and/or its Cognizant Security Office (e.g., Defense Counterintelligence and Security Agency).

(5) This requirement does not relieve the contractor from adhering to security incident guidance set forth by its Cognizant Security Office (e.g., Defense Counterintelligence and Security Agency).

(6) The contractor is responsible for ensuring all applicable subcontracts include these security incident reporting requirements.

(7) If the lost or compromised information is beyond the jurisdiction of the U.S. Government and cannot be recovered (e.g., media leak, public website posting, or loss in a foreign country), the notification and location of the compromise (e.g., geographic location of unrecoverable equipment) shall be classified commensurate with the classification level of the compromised material to prevent further unauthorized disclosure in accordance with DoDM5200.01 Volume 3, Enclosure 6. The contractor will contact the GCA for instructions on how to communicate the notification prior to submission in all cases where lost or compromised information is beyond the jurisdiction of the U.S. Government and cannot be recovered.

(8) The contractor shall ensure all notifications determined to contain classified information are properly transmitted and marked in accordance with derivative classification and overarching

marking guidelines in accordance with 32 CFR Part 117.

(b) Initial Notification of Security Incident

(1) The contractor shall provide an initial notification of security incident to the GCA within 72 hours of discovery of any incident where classified information may have been subjected to loss, compromise, or suspected compromise for all security incidents involving the contractor's location unless otherwise directed by contract requirements.

(2) The initial notification to the GCA is considered Controlled Unclassified Information (CUI) [CUI category OPSEC, FEDCON Distribution/Dissemination Control] unless otherwise determined by the GCA, marked in accordance with DoDI5200.48, and shall be transmitted to the GCA through authorized means (e.g., encrypted email or DoD SAFE).

(3) If the initial notification contains classified information either by content or through classification through compilation, the contractor will contact the GCA for submission guidance and ensure the notification is properly marked in accordance with derivative classification and overarching marking guidelines in accordance with 32 CFR Part 117.

(4) The initial notification shall contain the following information, as available at the time of report:

(i) Prime contract number associated with the security incident.

(ii) Date of security incident occurrence.

(iii) Date of security incident discovery if different from date of occurrence.

(iv) Security Classification Guide (SCG) or guidance used to validate classification level of information involved (unclassified title/date); if SCG title is either classified or if listing SCG information will cause the notification to be classified by compilation, do not include and indicate as such in the initial notification.

(v) Classification level of information involved (e.g., Top Secret, Secret, or Confidential)

(vi) Brief description of incident prompting initial notification. If incident directly or indirectly involved government personnel, include government personnel name(s), email address(s), and office information.

(vii) Communicate whether it is possible for the contractor to properly retain and/or provide the suspected information in question for GCA classification review and/or damage assessment.

(c) Final Notification of Security Incident

(1) The contractor shall provide a final notification to the GCA 10 business days from date of initial notification. If the final notification cannot be made 10 business days from the date of the initial notification, the contractor shall request an extension and receive approval in writing from the GCA.

(2) The final notification to the GCA does not relieve the contractor from reporting requirements set forth by 32 CFR Part 117, DFARS 252.204-7012, or as otherwise directed by contract requirements and/or its Cognizant Security Office (e.g., Defense Counterintelligence and Security Agency).

(3) The final notification will be considered CUI [CUI category OPSEC, FEDCON Distribution/Dissemination Control] unless otherwise determined by the GCA, marked in accordance

with DoDI5200.48, and sent through authorized means (e.g., encrypted email or DoD SAFE).

(4) If the final notification contains classified information either by content or through classification through compilation, the contractor is required to contact the GCA for submission guidance and ensure the notification is properly marked in accordance with derivative classification and overarching marking guidelines in accordance with 32 CFR Part 117.

(5) The final notification shall contain the following information:

(i) Prime contract number associated with the security incident.

(ii) Date of security incident occurrence.

(iii) Date of security incident discovery if different from date of occurrence.

(iv) Security Classification Guide (SCG) or guidance used to validate classification level of information involved (unclassified title/date); if SCG title is either classified or if listing SCG information will cause the report to be classified by compilation, do not include this information, and indicate as such in the final notification.

(v) Classification level of information involved (e.g., Top Secret, Secret, or Confidential)

(vii) Detailed description of incident and include the following:

Sequence of events: When, where, and how did the incident occur?

What persons, situations, and/or conditions caused or contributed to the incident?

If incident originated with government personnel, include government personnel name(s), email address(s), and office information.

Include the name(s), email address(s), and office information of all government personnel involved, either directly or indirectly, as appropriate

If classified information is alleged to have been physically lost (e.g., lost classified document), what steps were taken to locate the material?

If security incident was categorized as a data spill, include measures taken to properly sanitize all impacted assets.

(viii) Corrective actions taken to prevent future occurrences

(ix) Result of inquiry (e.g., loss, compromise, suspected compromise, or no compromise)

(x) A copy of the supporting DD Form 254(s) associated with prime contract. If DD Form 254 cannot be provided, the contractor shall indicate the reasons why in the final report.

(d) Definitions

“32 CFR Part 117” means National Industrial Security Program Operating Manual.

“Business days” means days that do not include federal holidays or weekends.

“Classified information” means information the government designates as requiring protection

against unauthorized disclosure in the interest of national security, pursuant to E.O. 13526, Classified National Security Information, or any predecessor order, and the Atomic Energy Act of 1954, as amended. Classified information includes national security information (NSI), restricted data (RD), and formerly restricted data (FRD), regardless of its physical form or characteristics (including tangible items other than documents).

“Cognizant security agencies (CSAs)” means agencies E.O. 12829, sec. 202, designates as having National Industrial Security Program implementation and security responsibilities for its own agencies (including component agencies) and any entities and non-CSA agencies under their cognizance. The CSAs are: Department of Defense (DoD); Department of Energy (DOE); Nuclear Regulatory Commission (NRC); Office of the Director of National Intelligence (ODNI); and Department of Homeland Security (DHS).

“Cognizant Security Office” means an organizational unit to which the head of a CSA delegates authority to administer industrial security services on behalf of the CSA.

“Compromise” means an unauthorized disclosure of classified information.

“Data spill” means electronic transmission of classified information via unsecure means such as classified information transmitted over an unclassified network.

“DD Form 254” means the Department of Defense Contract Security Classification Specification.

“Derivative classification” means incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

“Final Notification of Security Incident” means contractor (or subcontractor) notification to the Government Contracting Activity communicating the results of the inquiry conducted.

“Government Contracting Activity” means an element of a Component designated and delegated by the Component head or designee with broad authority regarding acquisition functions to include the appropriate resources and personnel (e.g., contracting officers or their designees, program managers, program offices, and security personnel) as defined in DoDM 5220.32, Volume 1.

“Initial Notification of Security Incident” means the contractor’s (or subcontractor) notification to the Government Contracting Activity of a security incident occurrence and surrounding details of occurrence.

“Inquiry” means the initial fact-finding and analysis process to determine the facts of any security incident and conducted to determine whether or not there was a loss of classified information or whether or not unauthorized personnel had, or could have had, access to the information.

“Loss” means the inability to physically locate or account for classified information.

“Security classification guide” means a documentary form of classification guidance issued by an Original Classification Authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

“Security Incident” means an incident that results from the mishandling of classified information.

“Suspected Compromise” means when a result of no loss or compromise of classified information cannot be determined with certainty.

(End of clause)

Parent topic: Subpart 5352.2 — TEXT OF PROVISIONS AND CLAUSES