Department of Energy
Under Secretary for Nuclear Security
Administrator, National Nuclear Security Administration
Washington, DC 20585

May 27, 2015

CERTIFIED MAIL
RETURN RECEIPT REQUESTED

Dr. Paul J. Hommert
President
Sandia Corporation
Sandia National Laboratories
1515 Eubank SE
Building 802 / Room 3180
Albuquerque, New Mexico 87123

SEA-2015-01

Dear Dr. Hommert:

This letter refers to the Department of Energy's (DOE) investigation into the facts and circumstances related to an incident of security concern (IOSC) regarding the unauthorized disclosure and introduction of classified information into unapproved information systems (security event) at the DOE's National Nuclear Security Administration (NNSA) Sandia National Laboratories (SNL). Based on the onsite investigation and evaluation of the evidence in this matter, and in consideration of information presented by Sandia Corporation (Sandia) officials during the enforcement conference on September 9, 2014, NNSA is issuing the enclosed Preliminary Notice of Violation (PNOV) to Sandia in accordance with 10 C.F.R. § 824.6, *Preliminary Notice of Violation*. A summary of the enforcement conference is also enclosed.

NNSA has determined that the unauthorized disclosure and introduction of classified information into unapproved information systems at SNL resulted in six violations of DOE classified information security requirements. Violations committed by Sandia include: (1) failure to adequately perform requisite classification reviews; (2) failure to protect and control classified information; (3) failure to use approved information systems to develop, store, and disseminate classified information; (4) failure to conduct an adequate and thorough IOSC inquiry; (5) failure to conduct a sufficient causal analysis and implement adequate corrective actions designed to prevent recurrence; and (6) failure to implement a comprehensive self-assessment process addressing the protection and control of classified information. Sandia security management deficiencies relating to the protection of classified information are detailed in the enclosed PNOV, which describes four Severity Level I violations, two Severity II violations, and proposes a total civil penalty of $577,500.

Pursuant to 10 C.F.R. § 824.4, *Civil penalties*, subsection (d), NNSA may assess a civil penalty for each day of a continuing violation. In consideration of the long-standing noncompliant conditions cited in this PNOV, which existed over a decade, NNSA has elected to cite violation (1) for two separate days. Each violation reflects the maximum applicable per-day base civil penalty authorized under 10 C.F.R. § 824.4(c) at the time of the security event.

Pursuant to 10 C.F.R. § 824.6(a)(4), Sandia has the right to submit a written reply within 30 calendar days of receipt of the enclosed PNOV. A reply must contain a statement of all relevant facts pertaining to the violations alleged, and must otherwise follow the requirements of 10 C.F.R. § 824.6(b). Pursuant to 10 C.F.R. § 824.6(c), failure to submit a written reply within 30 calendar days constitutes relinquishment of any right to appeal any matter in the PNOV; and the PNOV, including the civil penalty assessment, will constitute a final order.

After reviewing your response to the PNOV, including any proposed additional corrective actions, a determination will be made on whether further action is necessary to ensure Sandia's compliance with DOE's classified information security requirements.

Sincerely,

Frank G. Klotz

Enclosures: Preliminary Notice of Violation (SEA-2015-01)
Enforcement Conference Summary and List of Attendees

cc: Jeffrey Harrell, NNSA/SFO
Michael Hazen, Sandia
Gabriel King, Sandia

Preliminary Notice of Violation

Sandia Corporation
Sandia National Laboratories, New Mexico

SEA-2015-01

The U.S. Department of Energy (DOE) conducted an investigation into the facts and circumstances surrounding an incident of security concern (IOSC) regarding the unauthorized disclosure of classified information and the introduction of classified information into unapproved information systems that was discovered by a Sandia manager on July 31, 2012 (hereinafter referred to as the security event) at Sandia National Laboratories, New Mexico (SNL/NM), which is managed and operated for the DOE National Nuclear Security Administration (NNSA) by Sandia Corporation (Sandia).[1] Following the investigation, DOE issued an investigation report, *Unauthorized Disclosure of Classified Information and the Introduction of Classified Information into Unapproved Information Systems: Sandia National Laboratories, New Mexico, Sandia Corporation* (hereinafter referred to as the DOE investigation report) dated July 11, 2014, which was provided to Sandia on the same date.[2] On September 9, 2014, an enforcement conference, attended by DOE, NNSA, and Sandia representatives, was held at DOE Headquarters to discuss the findings of the DOE investigation report.[3]

The purpose of the DOE investigation was to evaluate the security event and to identify potential violations that could be subject to enforcement activity. The DOE investigation report identified six violations of DOE classified information security requirements that resulted in or were revealed by the security event. Violations committed by Sandia include: (1) failure to adequately perform requisite classification reviews; (2) failure to protect and control classified information; (3) failure to use approved information systems to develop, store, disseminate and control access to classified information; (4) failure to conduct an adequate and thorough IOSC inquiry; (5) failure to conduct a sufficient causal analysis and implement adequate corrective actions designed to prevent recurrence; and (6) failure to implement a comprehensive self-assessment process addressing the protection and control of classified information.

Pursuant to section 234B of the Atomic Energy Act of 1954 and DOE regulations set forth at 10 C.F.R. Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations,* NNSA hereby issues this Preliminary Notice

---

[1] DOE/NNSA Contract No. DE-AC04-94AL85000, awarded October 1, 1993 (Sandia Contract). The Sandia Contract subsequently has been modified.

[2] The DOE investigation report sets forth the findings that underlie the violations alleged in this Preliminary Notice of Violation.

[3] A summary of the enforcement conference is enclosed with this PNOV (Enforcement Conference Summary). During the enforcement conference, the Sandia Vice President for Infrastructure Operations and Chief Security Officer stated that Sandia did not object to the factual findings documented in the DOE investigation report.

of Violation (PNOV) to Sandia and proposes civil penalties for four Severity Level I violations of DOE classified information security requirements set forth in DOE Order 452.8, *Control of Nuclear Weapon Data* (July 21, 2011); DOE Order 475.2A, *Identifying Classified Information* (February 1, 2011); NNSA Policy (NAP) 70.4, Chg. 1, *Information Security* (July 2, 2010); and NAP 14.1-C, *NNSA Baseline Cyber Security Program* (May 2, 2008), and two Severity Level II violations of DOE classified information security requirements set forth in DOE Manual 470.4-1, Chg. 2, *Safeguards and Security Program Planning and Management* (October 20, 2010).[4]

Severity Level I violations are defined in 10 C.F.R. Part 824, Appendix A, *General Statement of Enforcement Policy*, paragraph V.b. as "violations [that] are reserved for classified information security requirements which involve the actual or high potential for adverse impact on the national security." Severity Level II violations are defined as "violations [that] represent a significant lack of attention or carelessness toward responsibilities of DOE contractors for the protection of classified information which could, if uncorrected, potentially lead to an adverse impact on the national security." The violations are identified below.

I. Violations

A. Failure to adequately perform requisite classification reviews

Title 10, C.F.R., Part 1045, *Nuclear Classification and Declassification*, section 1045.44, states that "[a]ny person with authorized access to [Restricted Data] RD or [Formerly Restricted Data] FRD who generates a document intended for public release in an RD or FRD subject area shall ensure that it is reviewed for classification by the appropriate DOE organization (for RD) or the appropriate DOE or DoD organization (for FRD) prior to its release".

DOE Order 452.8, *Control of Nuclear Weapon Data* (July 21, 2011), Attachment 1, *Contractor Requirements Document*, Section 6, Marking, paragraph 6.a, states that "all newly created [nuclear weapon data] … must be reviewed for Sigma 14, Sigma 15, Sigma 18 and /or Sigma 20 content and appropriately marked."

DOE Order 475.2A, *Identifying Classified Information* (February 1, 2011), Attachment 1, *Contractor Requirements Document*, Section 1, Requirements, paragraph 1.b, states that "[c]lassified information contained in documents or material must be correctly identified and appropriate classifier markings must be placed on the documents or material." Attachment 4, *Classification/Declassification Review Requirements*, Section 1, Classification, states that "[d]ocuments or material

[4] DOE Orders and Manuals, and NNSA policy statements are applicable to Sandia pursuant to the Sandia Contract, Part III – Section J, Clause I-72, DEAR 970.5204-2, Laws, Regulations and DOE Directives (DEC 2000), Appendix G, *List of Applicable Directives, and NNSA Policy Letters*. At the time of the security event, DOE O 452.8 and DOE O 475.2A were incorporated into Appendix G and continue to be so incorporated. DOE Manual 470.4-1, Chg. 2, NAP 70.4, and NAP 14.1-C were incorporated into Appendix G at the time of the security event; they are no longer incorporated in Appendix G as of the date of this PNOV.

potentially containing classified information must be reviewed for classification to ensure that such information is identified for protection." Attachment 4, paragraph 1.a.(1), states that "[n]ewly generated documents or material in a classified subject area and that potentially contain classified information must receive a classification review by a Derivative Classifier." Attachment 4, paragraph 1.a.(4), requires that "[d]ocuments or material in a classified subject area intended for public release (e.g. for a webpage, for Congress) must be reviewed by the Classification Officer."

NAP 70.4, *Information Security* (July 2, 2010), Section A, *Classified Matter Protection and Control*, Chapter II, *Classified Matter Protection and Control Requirements*, paragraph 1.a, states that "[t]he originator is responsible for obtaining a classification review by a derivative or original classifier if there are any questions regarding the classification of any draft document or working paper."

Contrary to these requirements, based on the following facts, Sandia failed to obtain requisite classification reviews for newly generated documents in a classified subject area and information in a classified subject area intended for public release.

1. On July 31, 2012, a Sandia manager discovered a presentation by a Sandia employee (hereinafter referred to as the author) containing classified information in the form of 13 information slides developed for the author's organization that were stored on an unclassified shared network server (hereinafter referred to as the 2012 presentation).[5] The inquiry subsequently conducted by Sandia (hereinafter referred to as the inquiry) determined that beginning as early as 1997 the author had developed approximately 47 separate variations of the 2012 presentation without obtaining requisite classification reviews.[6] As he was preparing his presentations, the author failed to ask the Sandia classification office to review them to determine if they contained classified information in accordance with applicable requirements. The Sandia classification office and DOE's Office of Classification determined that all 13 information slides contained classified information, including Confidential/ Formerly Restricted Data (C/FRD), Confidential/Restricted Data, Secret/Formerly Restricted Data, Secret/Restricted Data (S/RD), and Critical Nuclear Weapon Design Information (CNWDI).[7]

2. Sandia's inquiry further determined that the author also conducted classified presentations using variations of the 2012 presentation in unclassified settings at SNL/NM and, on at least three occasions, in public venues. Sandia's classification office was never asked by the author to conduct the required

---

[5] DOE investigation report, at 3.
[6] *Id.* Sandia reported the security event in the Safeguards and Security Information Management System (SSIMS) on August 2, 2012. Sandia's inquiry was conducted in three phases. Sandia's initial inquiry was opened on July 31, 2012, and formally closed on October 31, 2012. Upon receiving authorization from DOE, Sandia reopened its inquiry on April 10, 2013, and reported it as closed in SSIMS on March 7, 2014. Upon receiving authorization from DOE, on April 11, 2014, Sandia reopened its inquiry for the third time. Sandia reported the inquiry as closed in SSIMS on August 27, 2014.
[7] *Id.*

classification review of his presentations that contained classified information and were intended for public release.[8]

3. Sandia's inquiry also included the discovery that in July 2004, a version of the 2012 presentation and a video of the author conducting the presentation were uploaded onto an unclassified shared server.[9] A Sandia classification review in 2010 resulted in the removal of some of the classified information from the video presentation; however, at least one slide containing classified information (C/FRD) remained, and similar information was overlooked on the video.[10] Due to Sandia's failure to identify and remove all of the classified information contained in the presentation and the video, it remained stored and unprotected on this unclassified shared server for over eight years.[11]

Collectively, these noncompliances (Violation A) constitute a Severity Level I violation.
Base Civil Penalty - $110,000[12]
Proposed Civil Penalty - (as adjusted for escalation) - $220,000

B. Failure to protect and control classified information

DOE Order 452.8, *Control of Nuclear Weapon Data* (July 21, 2011), Attachment 1, *Contractor Requirements Document*, Section 4, Oral/Visual Communication, paragraph 4.a, states that "[o]ral/visual communications (e.g., discussions or presentations) must be restricted to those persons with appropriate [nuclear weapon data] clearance and valid need-to-know." Attachment 1, Section 5, Receiving and Transmitting, paragraph 5.a, states that "[d]istribution of [nuclear weapon data] within DOE (including NNSA and other locations) will be restricted to individuals with appropriate clearance and valid need-to-know."

NAP 70.4, *Information Security* (July 2, 2010), Section A, *Classified Matter Protection and Control*, Section 2, Requirements, paragraph 2.a, states that "[c]lassified matter that is generated, received, transmitted, used, stored, reproduced, permanently placed (buried according to the requirements of this NNSA Policy), or destroyed must be protected and controlled commensurate with classification level, category (if RD or FRD), and caveats (if applicable). All pertinent attributes must be used to determine the degree of protection and control required to prevent unauthorized access to classified matter."

---

[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.* at 3-4.
[12] 10 C.F.R. Part 824 was amended in 2009 to reflect that effective January 13, 2010, the maximum civil penalty per violation for Base Civil Penalty for Severity Level I violations was $110,000: 74 Fed. Reg. 66033 (December 14, 2009). This rule was amended again in 2014 to raise this figure to $120,000 effective February 3, 2014; 79 Fed. Reg. 1 (January 2, 2014). This rule adjusted DOE's civil monetary penalties for inflation as mandated by the Debt Collection Improvement Act of 1996. The 2009 change will be applied to the proposed Base Civil Penalties for Sandia because the security event was discovered in 2012.

Contrary to these requirements, based on the following facts, Sandia failed to protect and control classified information:

1. Sandia's inquiry revealed that the author developed approximately 47 separate variations of the 2012 presentation, all of which contained classified information.[13] It also revealed that between October 2003 and November 2011, different versions of the 2012 presentation were delivered on several occasions in unclassified settings at SNL/NM and on at least three occasions at public venues.[14] The audience for these presentations included individuals without security clearances, as well as individuals who had security clearances but lacked a need-to-know for the information being presented.[15]

2. Some of the presentations were supported by hard copy handouts, and electronic versions were frequently provided by the author upon request.[16] Approximately 300 Sandia participants in a technical training program had access to electronic versions of the presentations and, in at least one instance, participants received a set of unclassified compact disks containing a version of the 2012 presentation.[17] Since these media items were not appropriately marked to reflect classified contents, participants could e-mail the subject information to internal or external locations by unapproved means. Sandia's inquiry confirmed that at least one e-mail containing the 2012 presentation was sent to an external location by unapproved means.[18]

3. The DOE investigation confirmed that Sandia employees used a version of the 2012 presentation in developing their own presentations (which also contained classified information up to and including S/RD CNWDI) that could have resulted in additional compromises of classified information.[19]

Collectively, these noncompliances (Violation B) constitute a Severity Level I violation.
Base Civil Penalty - $110,000
Proposed Civil Penalty - $110,000

C. Failure to use approved information systems to develop, store, disseminate and control access to classified information

DOE Order 452.8, *Control of Nuclear Weapon Data* (July 21, 2011), Attachment 1, *Contractor Requirements Document*, Section 5, Receiving and Transmitting, paragraph 5.h, Electronic Transmission, states that "[n]on-Sigma [nuclear weapon

---

[13] DOE investigation report, at 3.
[14] *Id.* at 7.
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*

data] may be sent electronically only over approved classified networks if need-to-know for that information is assured."

NAP 70.4, *Information Security* (July 2, 2010), Section A, *Classified Matter Protection and Control*, Section 2, Requirements, paragraph 2.d, states that "[c]lassified information must only be processed on information systems that have received authority to operate according to NNSA Office of the Chief Information Officer directives that establish requirements for national security systems."

NAP 14.1-C, *NNSA Baseline Cyber Security Program* (May 2, 2008), Appendix C: CRD, page C-2, Section 6, Information Types/Groups, paragraph 6.a, states that "[a]ccess to classified information must be granted only to persons with the appropriate access authorization and Need-To-Know in the performance of their duties according to NNSA policies and DOE M 470.4-5, *Personnel Security*." Page C-8, Section 7, Responsibilities, paragraph 7.e.(4), requires the application owners/data stewards to "[e]nsure that the information is processed only on a system that is approved at a level appropriate to protect the information." Page C-9, Section 7, Responsibilities, paragraph 7.f.(8), requires that users "[e]nsure that system media and system output are properly classified, marked, controlled, and stored." Page C-9, Section 7, Responsibilities, paragraph 7.f.(11), requires that users "[o]bserve rules and regulations governing the secure operation and authorized use of information systems."

Contrary to these requirements, based on the following facts, Sandia (1) failed to ensure that classified information was processed, developed, stored, and disseminated only on approved information systems and servers; (2) failed to ensure that system media and output were properly classified, marked, controlled, and stored; and (3) permitted unauthorized access to classified information:

1. Beginning in 1997, the author created approximately 47 separate variations of the 2012 presentation that contained classified information (up to S/RD CNWDI) and were processed, developed, and disseminated on unapproved information systems located throughout SNL/NM.[20] Additionally, as early as 2003, the author also developed and stored these classified presentations on his personal computer and on an unapproved thumb drive.[21]

2. Although Sandia took immediate action to sanitize the unclassified shared network server upon discovery of the 2012 presentation stored on it, Sandia failed to conduct additional searches of other unapproved information systems to determine the extent of the problem.[22] For example, Sandia did not expand its search for additional presentations stored on other unclassified SNL/NM information systems and servers until eight months later.[23] The Sandia inquiry

[20] *Id.* at 3.
[21] *Id.* at 5.
[22] *Id.* at 9.
[23] *Id.*

report ultimately documented that approximately 47 variations of the 2012 presentation were eventually discovered in over 250 files on unapproved information systems located throughout SNL/NM.[24]

3. Many of these information systems containing variations of the 2012 presentation were accessible to individuals without security clearances and to others who had security clearances but without a need-to-know for the information being presented.[25] The Sandia inquiry confirmed that one of these contaminated Sandia unclassified servers was accessible to foreign nationals for over eight years.[26]

4. As of the conclusion of the DOE investigation in March 2014, Sandia was still reviewing all of its unclassified information systems to determine if other classified documents and files associated with the author and his organization were stored on such information systems.[27]

Collectively, these noncompliances (Violation C) constitute a Severity Level I violation.
Base Civil Penalty - $110,000
Proposed Civil Penalty - $110,000

D. Failure to conduct an adequate and thorough IOSC inquiry

DOE Manual 470.4-1, Chg. 2, *Safeguards and Security Program Planning and Management* (October 20, 2010), Attachment 2, *Contractors Requirements Document*, Part 2, *Safeguards and Security Management*, Section N, *Incidents of Security Concern*, paragraph 2.e, states that "[i]nquiries must be conducted to establish the facts and circumstances surrounding an incident of security concern."

Section N, Chapter I, *Identification and Reporting Requirements*, Section 6, Conduct of Inquiries, paragraph 6.b.(1-3) states that the following actions must be taken when conducting an IOSC inquiry:

(1) Data Collection:
- (a) Collect all data/information relevant to the incident, such as operation logs, inventory reports, requisitions, receipts, photographs, signed statements, etc.
- (b) Conduct interviews to obtain additional information regarding the incident.
- (c) Collect physical evidence associated with the inquiry, if available. (Examples of physical evidence include, but are not limited to, recorder charts, computer hard drives, defective/failed equipment, procedures, and readouts from monitoring equipment, etc.)
- (d) Ensure physical evidence is protected and controlled and a chain-of-custody is maintained.

---

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*

(2) Incident Reconstruction:
  (a) Reconstruct the incident of security concern to the greatest extent possible using collected information and other evidence.
  (b) Develop a chronological sequence of events that describes the actions preceding and following the incident.
  (c) Identify persons associated with the incident.
(3) Incident Analysis and Evaluation:
  (a) analyze the information collected during the inquiry to determine whether it describes the incident completely and accurately;
  (b) collect additional data and reconstruct the incident if more information is required;
  (c) identify any collateral impact with other programs or security interests.

Contrary to these requirements, based on the following facts, Sandia failed to conduct an adequate and thorough IOSC inquiry:

1. Sandia's inquiry was initiated on July 31, 2012, after the discovery of classified information within the 2012 presentation on an unclassified shared server.[28] Immediately after the discovery, Sandia transferred the 2012 presentation from the unclassified server to an approved classified server.[29] The contaminated unclassified server was sanitized, and a total of six hard drives connected to it were seized and identified for classified destruction.[30] However, as discussed below, because Sandia only searched for the author's work by the title of the 2012 presentation and not his name, classified versions of the 2012 presentation remained on the server. Further, no additional searches for the 2012 presentation were conducted outside of the author's organization during the first phase of the Sandia inquiry.[31]

2. During the first phase of its inquiry, Sandia determined that the author had worked on and stored the 2012 presentation on his personal computer and a thumb drive.[32] Sandia seized these items, but the Sandia inquiry official lacked the special equipment needed to inspect the electronic media without destroying the information on the computer or thumb drive. The inquiry official made no attempt to determine whether another organization within SNL/NM had the necessary equipment.[33] Consequently, the Sandia inquiry was initially closed in October 2012 without identifying additional classified presentations that were later found stored on the thumb drive.[34]

3. In March 2013, a Sandia employee assigned to the contractor's regulatory compliance organization conducted an independent query to validate that all

---

[28] *Id.* at 5.
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*

electronic versions of the 2012 presentation had been identified and affected information systems had been sanitized.[35] This query searched unclassified information systems using the author's name instead of the title of the 2012 presentation, and led to the discovery of the approximately 47 variations of the 2012 presentations by the author and other Sandia employees on a shared Sandia unclassified server that was accessible to individuals without requisite security clearances and/or need-to-know, including foreign nationals.[36]

4. In April 2013 (six months after the Sandia inquiry had been officially closed), Sandia attempted to review the content on the author's personal computer, but in the process damaged the computer's hard drive to the point that no information could be retrieved.[37] However, a review of the author's thumb drive revealed the 2012 presentation, as well as 12 additional presentations containing classified information.[38] Sandia then formally requested approval from the Headquarters Office of Security Assistance to reopen the inquiry that Sandia had closed in October 2012.[39] As explained above, during what became the second phase of the Sandia inquiry process Sandia discovered approximately 47 additional presentations containing classified information on unapproved information systems.[40]

5. In March 2014, just before the DOE investigation took place, Sandia again closed the inquiry. At that time, Sandia was still attempting to identify the full extent of the contamination and determine the appropriate path forward. After the DOE investigation, Sandia reopened its inquiry for the third time on April 11, 2014.[41]

Collectively, these noncompliances (Violation D) constitute a Severity Level I violation.
Base Civil Penalty - $110,000
Proposed Civil Penalty (as adjusted for mitigation) - $55,000

E. Failure to conduct a sufficient causal analysis and implement adequate corrective actions designed to prevent recurrence

DOE Manual 470.4-1, Chg. 2, *Safeguards and Security Program Planning and Management* (October 20, 2010), Attachment 2, *Contractor Requirements Document*, Part 2, *Safeguards and Security Management*, Section N, *Incidents of Security Concern*, paragraph 2.g, states that "[a]ppropriate corrective actions must be taken for each incident of security concern to reduce the likelihood of recurrence of the incident, including review and/or revision of applicable safeguards and security (S&S) plans and procedures."

---

[35] *Id.*
[36] *Id.* This was a different server than the server where the 2012 presentation was discovered on July 31, 2012.
[37] *Id.* at 6.
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] Sandia Inquiry Report, dated August 27, 2014.

Section N, Chapter I, Identification and Reporting Requirements, Section 6, Conduct of Inquiries, paragraph 6.b.(3) states that the following action must be taken when conducting an IOSC inquiry: "(3) Incident Analysis and Evaluation. This analysis determines which systems/functions performed correctly or failed to perform as designed. It provides the basis for determining the cause of the incident and subsequent corrective actions. Inquiry officials must: ... (c) identify any collateral impact with other programs or security interests."

Section N, paragraph 2.d states that "[l]ocally developed procedures must be established, documented, approved by the Departmental element, and disseminated to ensure the identification, reporting, root cause analysis, and resolution of incidents of security concern."

Contrary to these requirements, based on the following facts, Sandia failed to conduct a sufficient causal analysis and implement adequate corrective actions designed to prevent recurrence of the loss of classified information across SNL/NM:

1. Sandia National Laboratories Corporate Procedure CG100.6.9, *Conduct Root Cause Analysis and Extent of Condition Reviews*, requires that an extent-of-condition review determine whether other local operations may be at risk for the same problem.[42] The DOE investigation report determined that Sandia performed its first causal analysis in October 2012 in conjunction with the first phase of the Sandia inquiry, but the resulting corrective actions focused exclusively on the author's organization and did not include other Sandia organizations that also work with classified subject areas to determine if the 2012 presentation or variations of it were stored on their information systems.[43]

2. The extent-of-condition review portion of the Sandia causal analysis acknowledged the risk that other Sandia unapproved information systems may still contain multiple presentations that contain classified information.[44] However, the causal analysis team declined to pursue any further review of Sandia's electronic files to search for the 2012 presentation.[45] Instead, the causal analysis team made two recommendations: "(1) At the division level: perform a division wide self-assessment of these shared collaborative servers to verify that classified information does not exist on these servers by assessing a statistical sample of the number of sites and a statistical sample of a number of documents on each site; and (2) At the corporate level: perform a policy implementation assessment in fiscal year 2013 of these kinds of servers to verify that classified

---

[42] DOE investigation report, at 12.
[43] *Id.* Sandia conducted three extent-of-condition reviews. The first review was part of the causal analysis performed in October 2012 during the first phase of the Sandia inquiry. The second review was a part of Sandia's second causal analysis performed in September 2013 during the second phase of the Sandia inquiry. The third review was conducted after DOE's investigation, and completed in August 2014.
[44] *Id.*
[45] *Id.*

information does not exist on these servers, by assessing a statistical sample of the number of sites and a statistical sample of a number of documents on each site."[46]

3. The DOE investigation report determined that neither of these recommendations was acted upon after the initial causal analysis, and the conditions at other SNL/NM organizations were not reviewed until after the DOE investigation.[47] As a result, classified information in the form of various iterations of the 2012 presentation remained unprotected on unapproved information systems and was vulnerable to further unauthorized access from July 2012 until August 2014 when the Sandia inquiry was finally closed.[48]

4. The DOE investigation report determined that appropriate corrective actions were not implemented to prevent recurrence of classified information such as the 2012 presentation being placed on unapproved information systems for classified information.[49] The author's organization failed to recognize and adequately address the potential risk of the inappropriate disclosure of classified information, as evidenced by its decision to mark all questionable computer file presentations as Official Use Only (OUO).[50] The author's organization also decided to continue storing these presentations on an unapproved server until classification reviews could be completed.[51] As of the date of DOE's investigation, (March 2014) approximately 20 employees assigned to the author's organization were not aware of this arrangement. These employees therefore could create additional presentations based on the 2012 presentation and store them on unapproved information systems, believing the information to be OUO.[52]

5. Sandia implemented two corrective action plans, on October 2, 2012 and September 25, 2013, for the security event that primarily consisted of security awareness and lessons-learned activities and some procedural changes within the author's organization. They did not address the noncompliant conditions associated with the failure to conduct the requisite classification reviews and work planning and control that contributed to this security event (i.e., the placement of classified information on an unclassified server).[53] Both corrective action plans narrowly focused on the author's organization and therefore did not address potential problems concerning control of classified information at other SNL/NM organizations.[54]

---

[46] *Id.*
[47] *Id.*
[48] *Id.* At that point, the Sandia inquiry had been opened and closed for a third time, and Sandia represented to DOE that all of its unclassified information systems had been searched for the 2012 presentation and iterations thereof and no more had been found.
[49] *Id.*
[50] *Id.* at 12-13.
[51] *Id.* at 13. This is the same server where the 2012 Presentation was discovered on July 31, 2012.
[52] *Id.*
[53] *Id.*
[54] *Id.*

Collectively, these noncompliances (Violation E) constitute a Severity Level II violation.
Base Civil Penalty - $55,000
Proposed Civil Penalty - $55,000

F. Failure to implement a comprehensive self-assessment process addressing the protection and control of classified information

DOE Manual 470.4-1, Chg. 2, *Safeguards and Security Program Planning and Management* (10/20/2010), Attachment 2, Contractor Requirements Document, Part 1, Planning and Evaluations, Section G, Survey, Review, and Self-Assessment Programs, paragraph 1.a., states that the objective of the self-assessment program is to "[p]rovide assurance to the Secretary of Energy, Departmental elements, and other government agencies (OGAs) that safeguards and security (S&S) interests and activities are protected at the required levels." Paragraph 1.b. states that an additional objective is to "[p]rovide a basis for line management to make decisions regarding S&S program implementation activities, including allocation of resources, acceptance of risk, and mitigation of vulnerabilities. The results must provide a compliance-and-performance-based documented evaluation of the S&S program." Paragraph 2.b. states, in part, that "[s]urveys and self-assessments must provide an integrated evaluation of all topical and subtopical areas to determine the overall status of the S&S program and ensure that the objectives of this section are met." Subparagraph (3) states that "[c]omprehensiveness identifies the breadth of protection afforded all activities and interests within a facility. This is accomplished by an evaluation of the adequacy and effectiveness of programs and a thorough examination of the implementation of policies, practices, and procedures to ensure compliance and performance...."

Contrary to these requirements, based on the following facts, Sandia's self-assessments at the author's organization were not comprehensive and did not thoroughly evaluate the adequacy and effectiveness of activities related to the protection and control of classified information:

1. Sandia's procedures for conducting self-assessments are set forth in its Security Integrated Assessments (S&S-OP-199), Classified Matter Protection and Control Assessment Processes (S&S-OP-013), and Self-Assessment and Corrective Action Management procedure (S&S-SBS-004).[55] Assessments are conducted by a dedicated Sandia organization. The DOE investigation reviewed Sandia's May 2011 and November 2013 integrated assessments of the author's organization and found that these assessments identified no "findings" of problems with protection and control of classified information and only four "observations" on minor procedural discrepancies that were addressed on the spot.[56]

2. Sandia's November 2013 integrated assessment report identified three

[55] DOE investigation report, at 10. Sandia refers to some "self-assessments" as "integrated assessments".
[56] Integrated Assessments – *Weapon Engineering Professional Development,* dated May 23, 2011, and November 5, 2013.

classification "concerns" that were directly related to the failure to identify classified information in unclassified presentations created by the author and others.[57] These "concerns" were identified by Sandia as follows:

- "Some of the presentations have been used for several years, and although the presenters are encouraged to review the material prior to presentation, there is no record documenting such reviews."
- "The author's organization builds notebooks for the participants, so some of the presentations were released outside SNL/NM without undergoing the formal classification review and approval process."
- "Students also extract information from the Internet and other external sources to build their final presentations."[58]

3. The term "concern" is not defined in any of its integrated assessment procedures identified above.[59] As a result, these "concerns" were not recognized or entered into the Sandia issues management system, as would a finding or an observation.[60] The DOE investigation revealed that the author's organization failed to identify any of the noncompliant conditions that were eventually revealed by the security event. Although the Sandia integrated assessment program began in 2008, no findings were issued for any integrated assessment until March 2014.[61]

4. Only one of the two persons responsible for conducting the classification portion of the November 2013 integrated assessment of the author's organization had received any formal training as an assessor, such as that provided by the DOE National Training Center.[62] One assessor stated that she was new and never had the opportunity to be trained to perform assessments.[63] Both assessors indicated that there was no planning before the conduct of the November 2013 assessment and that they were only vaguely aware of the security incident that had occurred within the author's organization.[64]

5. During interviews with DOE investigators, the assessors said that the scope of the November 2013 assessment was time-limited by the Sandia assessment organization and could last no longer than six hours.[65] The assessors saw their role in the assessment process as primarily ensuring that derivative classifiers had access to the proper classification guidance and any other required resources.[66] Neither assessor indicated their role was to identify noncompliances or to perform assessment activities that would assist line management in understanding the

---

[57] DOE investigation report, at 10.
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] *Id.* at 11.
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*

effectiveness of the classification and information security programs.[67] When asked how they identified the concerns listed in the November 2013 integrated assessment report, the assessors said that this information came from an interview with one of the derivative classifiers in the author's organization.[68] The assessors could not explain why the identified "concerns" were not labeled as findings or observations, consistent with Sandia procedures which would require them to be entered into the Sandia issues management system, and tracked to conclusion.[69]

6. In addition to the integrated assessments, in April 2013 Sandia's assurance organization also conducted a classified matter protection and control assessment of classified procedures within the author's organization.[70] The assessment team conducted knowledge and performance tests; completed a checklist to confirm compliance with Sandia corporate policy 100.1, *Perform Classified Work*; and reviewed a sample of 35 classified documents for classification markings.[71] Only one minor error was identified, and no other findings or observations were noted. The overall rating was "Satisfactory."[72] The DOE investigation report determined that the April 2013 assessment activities conducted at the author's organization were limited in scope and lacked the rigor necessary to identify the noncompliant conditions revealed by the security event.[73] As a result, Sandia management had only a limited perspective on the effectiveness of the information security program for the author's organization and was relying on insufficient assessment results as a basis for line management decision-making on the effective implementation of classified information protection and control.[74]

Collectively, these noncompliances (Violation F) constitute a Severity Level II violation.
Base Civil Penalty - $55,000
Proposed Civil Penalty (as adjusted for mitigation) - $27,500

---

[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] CMPC Assessment Report, CWS 624, dated April 19, 2013. Assessment Report, CWS 624, dated April 19, 2013.
[71] *Id.*
[72] *Id.*
[73] DOE investigation report, at 11.
[74] *Id.*

II. Assessment of Civil Penalties

The significance of the classified information involved in the security event and the longstanding nature of the noncompliant conditions are primary factors in NNSA's determination of appropriate civil penalties. Sandia failed to conduct requisite classification reviews to ensure that classified information was appropriately identified and protected from unauthorized access. Sandia did not understand the full extent of the security event until August 2014, when the Sandia inquiry was finally completed. Sandia therefore failed to adequately protect and control classified information for more than a decade, beginning with the author's initial development of a presentation that contained classified information on unapproved information systems in 1997, until the completion of the inquiry process in August 2014.

A. Severity of the Violations

Both the Sandia inquiry report and the DOE investigation report concluded that a compromise of classified information occurred, that classified information was introduced into multiple unapproved information systems and servers, and that unauthorized individuals were given access to classified information up to and including S/RD CNWDI.[75] The security event resulted from the author's failure to obtain classification reviews for newly generated documents and information in a classified subject area. The subsequent development and storage of classified information on unapproved information systems, combined with the absence of adequate classification reviews, resulted in numerous instances of unauthorized access and the public release of classified information for more than a decade.[76]

The first phase of Sandia's inquiry lacked the necessary thoroughness to disclose additional versions of the 2012 presentation. Sandia did not expand its inquiry and begin to identify additional versions of the 2012 presentation stored in other unapproved information systems and servers for approximately five months after its inquiry initially was closed in October 2012.[77] Although during the first phase of its inquiry Sandia knew that the author had worked on and stored the 2012 presentation on his personal computer and a thumb drive, these items were not reviewed until approximately six months after closure of Sandia's inquiry.[78]

NNSA holds its contractors accountable for the acts of contractor employees who fail to follow classified information security requirements. The DOE investigation report determined that violations of classified information security requirements, as described above, have occurred. The security event resulted from a Sandia employee's failure to obtain required classification reviews and Sandia's failure to fully understand the extent of the classified information at risk and adhere to Departmental policies governing the identification, protection, and control of classified information.

---

[75] Sandia Inquiry Report, dated August 27, 2014 at 14.
[76] DOE investigation report, at 13.
[77] *Id.* at 5.
[78] *Id.*

B. Mitigation of Civil Penalties

NNSA provides strong incentives, through opportunity for mitigation, for contractors to self-identify and promptly report security noncompliances before a more significant adverse event or consequence arises. Sandia should have identified the security program weaknesses identified by the DOE investigation report before those weaknesses were revealed in July 2012. Classified information was developed, introduced into, and stored on unauthorized information systems; transmitted by unauthorized means; and improperly disclosed to unauthorized individuals on numerous occasions.[79] Upon discovery of the security incident, Sandia promptly reported it into SSIMS. However, Sandia failed to initially identify all of the unapproved information systems that contained classified information, leaving classified information at risk for an extended period of time.[80] Consequently, NNSA finds that no mitigation for self-identification and reporting is warranted.

Another mitigating factor considered by NNSA is the timeliness and effectiveness of contractor corrective actions. Upon discovery of the security event, Sandia took immediate corrective actions to contain and sanitize the known contaminated server within the author's organization.[81] However, Sandia made no additional effort to search other SNL/NM information systems for similar presentations addressing the same subject until approximately six months after closure of its initial inquiry. Additionally, an adequate extent-of-condition review mandated by DOE requirements was not initiated until after DOE's investigation, and was not completed until August 2014.[82] As a result, Sandia's initial corrective actions focused narrowly on the author's organization, rather than on broader weaknesses in Sandia's work control processes that allowed an employee to fail to seek required classification reviews for work in a classified subject area.[83] Consequently, NNSA finds that no mitigation for corrective actions involving violations A, B, C, and E is warranted.

Following the enforcement conference, Sandia provided documentation to DOE that described a number of significant improvements that have been implemented in its security incident management and self-assessment programs. This documentation stated that recent Sandia internal assessment activities identified 13 findings of noncompliances with requirements to protect and control classified information. As a result, NNSA finds that partial (50 percent) mitigation is warranted for corrective actions associated with violations D and F.

C. Civil Penalties

NNSA concludes that civil penalties are fully warranted in this case. While civil

---

[79] *Id.* at 8.
[80] *Id.* at 9.
[81] *Id.*
[82] *Id.*
[83] *Id.* at 12.

penalties assessed under 10 C.F.R. Part 824 should not be unduly confiscatory, they should be commensurate with the gravity of the violations at issue. In assessing penalties, NNSA considered the nature and severity of the violations in this case, as well as the circumstances in which they occurred.

Pursuant to 10 C.F.R. § 824.4, DOE may propose a civil penalty for each continuing violation on a per-day basis. NNSA has elected to assess the base civil penalty for Violation A for two separate days. This determination is based on the security significance of the classified information involved in the security event and Sandia's failure to conduct requisite classification reviews to ensure classified information was appropriately identified and protected for well over a decade.

In light of these considerations, NNSA proposes the imposition of a total civil penalty of $660,000 for the four Severity Level I violations and two Severity Level II violations, less 50 percent mitigation for corrective actions associated with Violations D and F, resulting in a total proposed civil penalty of $577,500.

III. Opportunity to Reply

Pursuant to 10 C.F.R. § 824.6(a)(4), Sandia may submit a written reply to this PNOV within 30 calendar days of receipt of the PNOV. Sandia may submit a request for a reasonable extension of time to file a reply to the Director, Office of Enforcement, in accordance with 10 C.F.R. § 824.6(d). The reply should be clearly marked as a "Reply to the Preliminary Notice of Violation."

If Sandia disagrees with any aspect of this PNOV or the proposed remedy, then as applicable and in accordance with 10 C.F.R. § 824.6(b), the reply shall: (1) state any facts, explanations, and arguments that support a denial of an alleged violation; (2) demonstrate any extenuating circumstances or other reason why the proposed remedy should not be imposed or should be further mitigated; and (3) discuss the relevant authorities that support the position asserted, including rulings, regulations, interpretations, and previous decisions issued by DOE. In addition, 10 C.F.R. § 824.6(b) requires that the reply include copies of all relevant documents.

If Sandia chooses not to contest the violations set forth in this PNOV and the proposed remedy, then the reply should state that Sandia waives the right to contest any aspect of this PNOV and the proposed remedy. In such case, the total proposed civil penalty of $577,500 must be remitted within 30 calendar days after receipt of this PNOV by check, draft, or money order payable to the Treasurer of the United States (Account 891099) and mailed to the address provided below. This PNOV will constitute a final order upon the filing of the reply.

Please send the appropriate reply by overnight carrier to the following address:

Director, Office of Enforcement
Attention: Office of the Docketing Clerk
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874-1290

A copy of the reply should also be sent to my office and the Manager of the NNSA Sandia Field Office.

Pursuant to 10 C.F.R. § 824.6(c), if Sandia fails to submit a written reply within 30 calendar days of receipt of this PNOV, Sandia relinquishes any right to appeal any matter in this PNOV, and this PNOV, including the proposed remedy, will constitute a final order.

Frank G. Klotz
Under Secretary for Nuclear Security
Administrator, NNSA

Washington, DC
This 27 day of May, 2015