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

July 13, 2015

VIA OVERNIGHT CARRIER

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

SEA-2015-01 (FNOV)

Dear Dr. Hommert:

Pursuant to section 234B of the Atomic Energy Act of 1954, as amended, (the Act) 42 U.S.C. § 2282b, and the Department of Energy (DOE) regulations at 10 C.F.R. Part 824, the National Nuclear Security Administration (NNSA) is issuing this Final Notice of Violation (FNOV) to Sandia Corporation (Sandia) for multiple violations of classified information security requirements. The FNOV is based upon DOE's investigation and an evaluation of the evidence presented to DOE by Sandia, including Sandia's final inquiry report, corrective actions, and Reply dated June 12, 2015, to the Preliminary Notice of Violation (PNOV) dated May 27, 2015. For the reasons set forth in the enclosed FNOV, NNSA finds no basis for modification of the PNOV. In accordance with 10 C.F.R. § 824.4, the FNOV imposes a civil penalty of $577,500.

All classified information requires a specified level of protection, commensurate with the classification level, until DOE determines the information to be unclassified. Sandia is aware of existing processes in place to have information declassified and approved for use in presentations or other use and retention. Thus, Sandia's assertion that because this classified information was in open sources, its unauthorized disclosure could not adversely impact national security, is not compliant with Departmental policy. If Sandia does not obtain the requisite classification reviews of information in classified subject areas, significant security incidents involving classified information are likely to recur at Sandia National Laboratories.

Pursuant to 10 C.F.R. § 824.7(b), Sandia has the right to submit to the Director of the Office of Enforcement, within 30 calendar days of the receipt of the FNOV, a written request for a hearing under § 824.8 or, in the alternative, to elect the procedures specified in section 234A.c.(3) of the Act, 42 U.S.C. § 2282a.(c)(3).

Sincerely,

Frank G. Klotz

Enclosure: Final Notice of Violation - SEA-2015-01 (FNOV)

cc: Jeffrey Harrell, NA-SN
Michael Hazen, Sandia
Gabriel King, Sandia

Final Notice of Violation

Sandia Corporation
Sandia National Laboratories, New Mexico

SEA-2015-01 (FNOV)

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 systems (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 the "DOE investigation report") dated July 11, 2014, which was provided to Sandia on the same date.[2] The DOE investigation report identified multiple violations by Sandia of DOE classified information security requirements.

On May 27, 2015, NNSA issued a Preliminary Notice of Violation (PNOV) to Sandia with a total proposed civil penalty of $577,500 for four Severity Level I violations of DOE classified information security requirements contained 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).[3]

---

[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 identified in this Final Notice of Violation.

[3] 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 (December 2000), Appendix G, *List of Applicable Directives, and NNSA Policy Letters*. At the time of the security event, DOE Order 452.8 and DOE Order 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 the FNOV.

NNSA received Sandia's Reply to the PNOV dated June 12, 2015, on June 16, 2015 (hereinafter the Reply). In the Reply, Sandia acknowledged that the six violations detailed in the PNOV did occur.[4] However, Sandia challenged NNSA's assessment of Severity Level I for Violations A, B, C, and D and Severity Level II for Violations E and F, on the basis that the information associated with the security event is available in open sources and could not result in any actual or high potential for adverse impact on national security.[5]

After thoroughly considering Sandia's Reply, NNSA finds no merit in the challenge to its determination of the severity level characterization for the six violations. Sandia's Reply did not set forth relevant facts pertaining to the violation to demonstrate that the significant and longstanding classified information security, cyber security, and other related noncompliances disclosed by the security event do not meet the severity level definitions in 10 C.F.R. Part 824, Appendix A, *General Statement of Enforcement Policy*, paragraph V.b.

The DOE Office of Classification has determined that the Sandia 2012 presentation (in which the classified information in question was found) contained classified information that included Confidential/Formerly Restricted Data (C/FRD), Confidential/Restricted Data (C/RD), Secret/Formerly Restricted Data (S/FRD), Secret/Restricted Data (S/RD), and CNWDI.[6] Additionally, as part of a systematic review process established by the DOE Office of Classification, some of the specific classified information contained in the 2012 presentation was further reviewed as recently as 2013 by subject matter experts from across the national laboratories, including a representative from Sandia. The results of that review confirmed that the information should and does remain classified at the levels defined in existing DOE classification guides.

Sandia asserted in its Reply that because DOE did not conduct a damage assessment, the assigned severity levels are without support and unsustainable.[7] The determination of severity levels assigned to violations of classified information security requirements pursuant to 10 C.F.R. Part 824 is not contingent on a damage assessment. Rather, a number of factors (e.g., classification level, information determined to be compromised, duration of the noncompliant conditions, etc.) are considered when assigning severity levels to confirmed violations. The relative weight given to each of these factors in arriving at the

---

[4] Sandia Corporation Reply to Preliminary Notice of Violation (SEA-2015-01)(Reply), at 2.
[5] *Id.* at.3.
[6] DOE investigation report, at 3.
[7] Reply, at 2.

appropriate severity level will depend on the circumstances of each case.[8] Both Sandia's inquiry and DOE's investigation determined that Sandia's failure to perform the required classification review of presentations in a classified subject area resulted in a number of unauthorized disclosures (i.e., compromises) of classified information at the Secret and Confidential levels[9] through various means (e.g., electronic, hard copy, verbal).[10] Thus, NNSA has concluded that Violations A, B, C, and D involve actual or high potential for adverse impact on the national security and Violations E and F represent a significant lack of attention or carelessness toward the protection of classified information, which could if uncorrected, potentially lead to an adverse impact on the national security.

Sandia further asserts that because the information disclosed by the security event was available in open sources, none of the Severity Level I violations could have involved an actual or high potential for adverse impact on national security, and that none of the Severity Level II violations could potentially have adversely affected national security.[11] The availability of this information in the open literature does not automatically declassify the information. DOE has a formal process for challenging the continued classification of information, but to date, Sandia has not pursued this process for the classified information in question. DOE's no-comment policy further provides that commenting on classified information in open literature can pose a risk of greater damage to national security by confirming its location, classified nature, or technical accuracy.[12] As a result of the publication and widespread dissemination of these presentations, Sandia has confirmed the technical accuracy of classified information in the public domain and provided credibility to the information being presented. Sandia's disclaimer referenced in its Reply does not conform to any recognized Departmental process or policy and does not relieve Sandia of the responsibility to identify, protect, and control classified information.[13]

Furthermore, the security event resulted from a Sandia employee developing variations of a presentation addressing a classified subject area for over 15 years without receiving the requisite classification review. DOE requires that all newly

---

[8] 10 C.F.R. Part 824, Appendix A, *General Statement of Enforcement Policy*, para V.e.
[9] 32 C.F.R. 2400.6, *Classification Levels*.
[10] DOE investigation report, at 3-4.
[11] Reply, at 3-4.
[12] 10 C.F.R. § 1045.22, *No Comment Policy*; DOE Classification Bulletin, GEN-16: "*No Comment Policy" on Classified Information in the Public Domain*, dated August 31, 2011; and DOE Classification Bulletin, GEN-16 Revision 2: "*No Comment" Policy on Classified Information in the Open Literature*, dated September 23, 2014.
[13] Reply, at 3.

generated documents in a classified subject area that may contain classified information, no matter the source (e.g., Internet or another open source), must receive a classification review by a Derivative Classifier or the Classification Officer.[14] Regrettably, the 2012 presentation, as well as other presentations containing similar classified information, were accessible to several Sandia employees familiar with the classified subject area, but none of those employees questioned the classified contents or sought a classification review over this extended period of time.

For the foregoing reasons, NNSA has determined that the enforcement action against Sandia as detailed in the PNOV shall remain unchanged. Pursuant to 10 C.F.R. § 824.7(b), NNSA hereby issues this Final Notice of Violation (FNOV) to Sandia for four Severity Level I violations and two Severity Level II violations of DOE's classified information security requirements as set forth below.

I. VIOLATIONS

A. Failure to adequately perform requisite classification reviews

Title 10, Code of Federal Regulations, 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,

[14] DOE Order 475.2A, Attachment 4, paragraph 1.a.(1).

Classification, states that "[d]ocuments or material 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).[15] 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.[16] 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

[15] DOE investigation report, at 3.

[16] *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.

and DOE's Office of Classification determined that all 13 information slides contained classified information, including C/FRD, C/RD, S/FRD, S/RD, and CNWDI.[17]

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 classification review of his presentations that contained classified information and were intended for public release.[18]

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.[19] 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.[20] 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.[21]

Collectively, these noncompliances (Violation A) constitute a Severity Level I violation.
Base Civil Penalty - $110,000[22]
Civil Penalty - (as adjusted for escalation) - $220,000

---

[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.* at 3-4.
[22] 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.

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."

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.[23] 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.[24] 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.[25]

2. Some of the presentations were supported by hard copy handouts, and electronic versions were frequently provided by the author upon request.[26] Approximately 300 Sandia participants in a technical training program had

[23] DOE investigation report, at 3.
[24] *Id.* at 7.
[25] *Id.*
[26] *Id.*

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.[27] 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.[28]

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.[29]

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

---

[27] *Id.*
[28] *Id.*
[29] *Id.*

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.[30] Additionally, as early as 2003, the author also developed and stored these classified presentations on his personal computer and on an unapproved thumb drive.[31]

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.[32] 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.[33] The Sandia inquiry report ultimately documented that approximately 47 variations of the 2012 presentation

[30] *Id.* at 3.
[31] *Id.* at 5.
[32] *Id.* at 9.
[33] *Id.*

were eventually discovered in over 250 files on unapproved information systems located throughout SNL/NM.[34]

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.[35] The Sandia inquiry confirmed that one of these contaminated Sandia unclassified servers was accessible to foreign nationals for over eight years.[36]

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.[37]

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

---

[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*

(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.

(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.[38] Immediately after the discovery, Sandia transferred the 2012 presentation from the unclassified server to an approved classified server.[39] The contaminated unclassified server was sanitized, and a total of six hard drives connected to it were seized and identified for classified destruction.[40] 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

[38] *Id.* at 5.
[39] *Id.*
[40] *Id.*

conducted outside of the author's organization during the first phase of the Sandia inquiry.[41]

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.[42] 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.[43] Consequently, the Sandia inquiry was initially closed in October 2012 without identifying additional classified presentations that were later found stored on the thumb drive.[44]

3. In March 2013, a Sandia employee assigned to the contractor's regulatory compliance organization conducted an independent query to validate that all electronic versions of the 2012 presentation had been identified and affected information systems had been sanitized.[45] 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.[46]

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.[47] However, a review of the author's thumb drive revealed the 2012 presentation, as well as 12 additional presentations containing classified information.[48] Sandia then formally requested approval from the Headquarters Office of Security

---

[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.* This was a different server than the server on which the 2012 presentation was discovered on July 31, 2012.
[47] *Id.* at 6.
[48] *Id.*

Assistance to reopen the inquiry that Sandia had closed in October 2012.[49] 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.[50]

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.[51]

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

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."

---

[49] *Id.*
[50] *Id.*
[51] Sandia Inquiry Report, dated August 27, 2014.

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.[52] 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.[53]

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.[54] However, the causal analysis team declined to pursue any further review of Sandia's electronic files to search for the 2012 presentation.[55] 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 information does not exist on these servers,

---

[52] DOE investigation report, at 12.

[53] *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.

[54] *Id.*

[55] *Id.*

by assessing a statistical sample of the number of sites and a statistical sample of a number of documents on each site."[56]

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.[57] 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.[58]

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.[59] 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).[60] The author's organization also decided to continue storing these presentations on an unapproved server until classification reviews could be completed.[61] 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.[62]

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

---

[56] *Id.*
[57] *Id.*
[58] *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.
[59] *Id.*
[60] *Id.* at 12-13.
[61] *Id.* at 13. This is the same server where the 2012 Presentation was discovered on July 31, 2012.
[62] *Id.*

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).[63] 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.[64]

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

---

[63] *Id.*
[64] *Id.*

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).[65] 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.[66]

2. Sandia's November 2013 integrated assessment report identified three classification "concerns" that were directly related to the failure to identify classified information in unclassified presentations created by the author and others.[67] 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."[68]

3. The term "concern" is not defined in any of its integrated assessment procedures identified above.[69] As a result, these "concerns" were not recognized or entered into the Sandia issues management system, as would a finding or an observation.[70] The DOE investigation revealed that the author's organization failed to identify any of the noncompliant

---

[65] DOE investigation report, at 10. Sandia refers to some "self-assessments" as "integrated assessments".
[66] Integrated Assessments – *Weapon Engineering Professional Development,* dated May 23, 2011, and November 5, 2013.
[67] DOE investigation report, at 10.
[68] *Id.*
[69] *Id.*
[70] *Id.*

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.[71]

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.[72] One assessor stated that she was new and never had the opportunity to be trained to perform assessments.[73] 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.[74]

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.[75] 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.[76] Neither assessor indicated their role was to identify noncompliances or to perform assessment activities that would assist line management in understanding the effectiveness of the classification and information security programs.[77] 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.[78] 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.[79]

6. In addition to the integrated assessments, in April 2013 Sandia's assurance organization also conducted a classified matter protection and control

---

[71] *Id.*
[72] *Id.* at 11.
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*

assessment of classified procedures within the author's organization.[80] 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.[81] Only one minor error was identified, and no other findings or observations were noted. The overall rating was "Satisfactory."[82] 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.[83] 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.[84]

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

II. DETERMINATION OF CIVIL PENALTIES

The significance of the classified information involved in the security event and the longstanding nature of the noncompliant conditions are the primary factors in NNSA's determination of appropriate civil penalties. NNSA imposes civil penalties for violations identified in Section I of this FNOV because of Sandia's failure to conduct requisite classification reviews to ensure classified information is 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.

---

[80] CMPC Assessment Report, CWS 624, dated April 19, 2013. Assessment Report, CWS 624, dated April 19, 2013.
[81] *Id.*
[82] *Id.*
[83] DOE investigation report, at 11.
[84] *Id.*

A. Severity Level 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.[85] 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 public release of classified information for more than a decade.[86] 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.[87] 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.[88]

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.

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

---

[85] Sandia Inquiry Report, dated August 27, 2014 at 14.
[86] DOE investigation report, at 13.
[87] *Id.* at 5.
[88] *Id.*

information was developed, introduced into, and stored on unauthorized information systems; transmitted by unauthorized means; and improperly disclosed to unauthorized individuals on numerous occasions.[89] Upon discovery of the security incident, Sandia promptly reported it in 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.[90] Consequently, NNSA finds that Sandia is not entitled to mitigation for self-identification and reporting.

Another mitigating factor considered by NNSA is the timeliness and effectiveness of contractor corrective actions. NNSA acknowledges Sandia's immediate corrective actions to contain and sanitize the known contaminated server within the author's organization.[91] 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 applicable DOE requirements was not initiated until after DOE's investigation, and was not completed until August 2014.[92] 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.[93] Consequently, NNSA finds that no mitigation is warranted for corrective actions involving violations A, B, C, and E.

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 Penalty Assessment

NNSA concludes that the civil penalty assessed in the PNOV is fully warranted in this case. While civil penalties assessed under 10 C.F.R. Part 824 should not be

---

[89] *Id.* at 8.
[90] *Id.* at 9.
[91] *Id.*
[92] *Id.*
[93] *Id.* at 12.

unduly confiscatory, they should be commensurate with the gravity of the violations at issue. In this regard, NNSA considered the nature and severity of the violations identified here, as well as the circumstances of the case.

Pursuant to 10 C.F.R. § 824.4(d), DOE may propose a civil penalty for each continuing violation on a per-day basis. NNSA has elected to impose the base civil penalty for Violation A for two separate days. In light of these considerations, NNSA imposes 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 civil penalty of $577,500.

III. Required Response

Pursuant to 10 C.F.R. § 824.7(d)(2), Sandia must, within 30 calendar days of receipt of this FNOV, submit to the Director of the Office of Enforcement one of the following:

(a) A waiver of further proceedings;

(b) A request for an on-the-record hearing under 10 C.F.R. § 824.8; or

(c) A notice of intent to proceed under section 234A.c.(3) of the Atomic Energy Act of 1954, as amended (42 U.S.C. § 2282a.(c)(3)).

Sandia's response to the FNOV shall be directed via overnight carrier to the following address:

Director, Office of Enforcement
Attention: Office of the Docketing Clerk, EA-10
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874-1290

A copy of any response should also be sent to the Manager of the Sandia Field Office, and to my office. The response shall be clearly marked as a "Response to a Final Notice of Violation."

If Sandia submits a waiver of further proceedings, the FNOV shall be deemed a final order enforceable against Sandia. Sandia shall submit payment of the civil penalty within 60 days of the filing of waiver unless additional time is granted by the Director, Office of Enforcement. The civil penalty shall be paid by check,

draft, or money order payable to the Treasurer of the United States (Account 891099) and mailed to the address provided above.

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

Washington, D.C.
this 13th day of July 2015