



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



September 26, 2014

CERTIFIED MAIL  
RETURN RECEIPT REQUESTED

Raymond J. Juzaitis, PhD  
President  
National Security Technologies, LLC  
Nevada National Security Site  
2621 Losee Road  
N. Las Vegas, Nevada 89030

SEA-2014-02

Dear Dr. Juzaitis:

This letter refers to the Department of Energy's (DOE) investigation into the facts and circumstances related to an incident of security concern regarding the unauthorized disclosure and introduction of classified information into unapproved information systems (security event) at the Department of Energy's National Nuclear Security Administration (NNSA) Nevada National Security Site (NNSS). Based on the onsite investigation and evaluation of the evidence in this matter, and in consideration of information presented by you and other National Security Technologies, LLC (NSTec) officials during the enforcement conference on July 16, 2013, NNSA is issuing the enclosed Preliminary Notice of Violation (PNOV) to NSTec 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 NNSS resulted in four violations of DOE classified information security requirements. Violations committed by NSTec include: (1) failure to obtain a requisite classification review; (2) failure to process classified information on approved information systems and maintain cyber sanitization documentation; (3) failure to conduct an adequate incident of security concern inquiry; and (4) failure to protect and control classified information. NSTec security management deficiencies relating to the protection of classified information are detailed in the enclosed PNOV, which includes four Severity Level II violations and a total proposed civil penalty of \$110,000. NNSA finds that mitigation for corrective action development and implementation is warranted (as discussed in Section II of the PNOV) for each



violation. Consequently, the maximum applicable per day base civil penalty for a Severity Level II citation authorized under 10 C.F.R. § 824.4(c) at the time of the security event has been mitigated by 50 percent.

Pursuant to 10 C.F.R. § 824.6(a)(4), NSTec 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 alleged violations 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 NSTec's compliance with DOE classified information security requirements.

Sincerely,



Frank G. Klotz

Enclosures: Preliminary Notice of Violation  
Enforcement Conference Summary

cc: Steven Lawrence, NA-NV  
Brian Barbero, NSTec  
Devin Biniaz, NSTec

## Preliminary Notice of Violation

National Security Technologies, LLC  
Nevada National Security Site

SEA-2014-02

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 storage, processing, and transmission of classified information (security event) at the Nevada National Security Site (NNSS), which is managed and operated for the DOE National Nuclear Security Administration (NNSA) by National Security Technologies, LLC (NSTec).<sup>1</sup> Following the investigation, DOE issued an investigation report, *Classified Information Introduced into Unapproved Systems and Locations: National Security Technologies, LLC* (Investigation Report) dated May 8, 2013, which was provided to NSTec on the same date.<sup>2</sup> On July 16, 2013, an enforcement conference, attended by DOE, NNSA, and NSTec representatives, was held at NNSS to discuss the findings of the Investigation Report.<sup>3</sup>

The purpose of the DOE investigation was to evaluate the security event and to identify potential violations that could be subject to an enforcement action. The Investigation Report identified four security violations of DOE classified information security requirements that resulted in the security event. Violations committed by NSTec include: (1) failure to obtain a requisite classification review; (2) failure to process classified information on approved information systems and maintain cyber sanitization documentation; (3) failure to conduct an adequate IOSC inquiry; and (4) failure to protect and control classified information from unauthorized disclosure.

Pursuant to section 234B of the Atomic Energy Act of 1954, as amended, and DOE regulations set forth at 10 C.F.R. Part 824, NNSA hereby issues this Preliminary Notice of Violation (PNOV) to NSTec and proposes a civil penalty for four Severity Level II violations of DOE classified information security requirements set forth in 10 C.F.R. Part 1045, *Nuclear Classification and Declassification*; DOE Order 475.2A, *Identifying Classified Information* (February 1, 2011); NNSA Policy Letter (NAP) 70.4, *Information Security* (July 2, 2010); DOE Manual 205.1-5, Chg. 2, *Cyber Security Process Requirements Manual* (December 22, 2009); DOE Manual 205.1-6, Chg. 2, *Media Sanitization Manual* (December 22, 2009); NAP 14.1-C, *NNSA Baseline Cyber Security*

---

<sup>1</sup> DOE/NNSA Contract No. DE-AC52-06NA25946, awarded March 28, 2006 (NSTec Contract). The NSTec Contract subsequently has been modified.

<sup>2</sup> The Investigation Report sets forth the investigative findings that underlie the violations asserted in this Preliminary Notice of Violation (PNOV).

<sup>3</sup> A summary of the enforcement conference is enclosed with the transmittal letter to this PNOV (Enforcement Conference Summary). During the enforcement conference, the NSTec Vice President for Program Integration stated that NSTEC did not take factual issue with the Investigation Report.

*Program* (May 2008); and DOE Manual 470.4-1, Chg. 2, *Safeguards and Security Program Planning and Management* (October 20, 2010).<sup>4</sup>

Severity Level II violations are defined in 10 C.F.R. Part 824, Appendix A, *General Statement of Enforcement Policy*, paragraph V.b. 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 a requisite classification review

Title 10 C.F.R. Part 1045, *Nuclear Classification and Declassification*, Subpart B, *Identification of Restricted Data and Formerly Restricted Data Information*, 10 C.F.R. § 1045.14 (a)(1) (2013), *Process for classification and declassification of restricted data and formerly restricted data information*, states that “[a]ny authorized holder who believes he or she has information which may be RD shall submit it to a RD classifier for evaluation....”

DOE Order 475.2A, Attachment 1, Contractor Requirements Document, Paragraph 1., *Requirements*, subparagraph b., requires 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.”

In addition, Attachment 4, Classification/Declassification Review Requirements, Paragraph 1., *Classification*, requires that “[d]ocuments or material potentially containing classified information must be reviewed for classification to ensure that such information is identified for protection.” Subparagraph a., *Required Classification Reviews*, (1) requires 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.”

Contrary to these requirements, based on the following facts, NSTec failed to obtain the requisite classification review for newly generated documents in a classified subject area.

1. In October 2011, an NSTec radiological control technician performing occupational radiation protection surveys for a classified activity that took place

---

<sup>4</sup> The DOE regulations, DOE Order and Manuals, and NNSA Policy Letters are applicable to NSTec pursuant to the NSTec Contract Part III – Section J, Section I Clause – DEAR 970.5204-2, Laws, Regulations and DOE Directives (DEC 2000), Appendix C, *List of Applicable Laws, Regulations and DOE Directives*. DOE Manual 205.1-5, Chg. 2; DOE Manual 205.1-6, Chg. 2 were incorporated into Appendix C at the time of the security event; they are no longer incorporated in Appendix C as of the date of issuance of this PNOV.

in 2011 questioned whether the information recorded on NSTec Form FRM-0108A, *Radiological Survey Report - MAP*, Rev 0, dated May 24, 2010 (hereafter referred to as the “survey form”), which was pre-marked as unclassified controlled nuclear information (UCNI), should be classified at the Secret/Restricted Data (S/RD) level and category.<sup>5</sup> The program manager for the classified activity, who was a derivative classifier/reviewing official, agreed that the information was S/RD.<sup>6</sup> The security event was discovered when the NSTec classification officer reviewed the subject survey form and confirmed that the information contained on the survey form was, in fact, S/RD.<sup>7</sup>

2. In accordance with NSTec standard operating procedure SOP-0441.211, dated June 16, 2011, radiological control technicians are required to document survey activities on a survey form.<sup>8</sup> The DOE investigation found that NSTec’s standard operating procedure failed to require a classification review for survey forms that are associated with a classified activity.
3. The DOE investigation further revealed that in early 2010, NSTec device assembly facility (DAF) radiological control technicians inquired about having the survey forms pre-marked as UCNI, including a completed reviewing official stamp.<sup>9</sup> The request was initiated because reviewing officials traditionally considered the survey information recorded on these forms to be UCNI.<sup>10</sup> Based on the NSTec radiological control technicians’ request, the NSTec radiological control department discussed the possibility of using pre-marked UCNI survey forms with the NSTec classification office.<sup>11</sup> The NSTec classification officer stated that the survey form could not be pre-marked UCNI, especially with a completed reviewing official stamp.<sup>12</sup> The classification officer further explained that an authorized derivative classifier/reviewing official had to review each survey form and mark it appropriately according to the classification determination.<sup>13</sup> Contrary to this advice, in May 2010, the NSTec radiological control supervisor directed the NSTec radiological control department to create a survey form pre-marked UCNI on the top and bottom of each page, but without the reviewing official stamp.<sup>14</sup>
4. In addition, the DOE investigation found that the radiological control technicians initially attempted to have the pre-marked UCNI survey forms reviewed, but authorized derivative classifiers/reviewing officials were unavailable.<sup>15</sup> As a

---

<sup>5</sup> Investigation Report, *supra* note 2, at 2.

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

<sup>8</sup> *Id.* at 2.

<sup>9</sup> *Id.*

<sup>10</sup> *Id.* at 2.

<sup>11</sup> *Id.* at 2-3.

<sup>12</sup> *Id.* at 3.

<sup>13</sup> *Id.*

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*

result, the radiological control technicians used the pre-marked UCNI survey forms, assuming that the information being recorded on the forms contained only UCNI information even when the survey work was being conducted for activities in a classified subject area.<sup>16</sup> Consequently, those completed survey forms never received the requisite classification review and, in some cases, were inappropriately marked and not protected or controlled as required for classified information.<sup>17</sup>

5. After NSTec discovered the security event in October 2011, it identified an additional classification issue in survey forms generated during a similar classified activity that took place at NNSS in 2009.<sup>18</sup> Upon further review, NSTec verified that the survey forms generated in 2009 also had not received the requisite classification review.<sup>19</sup> Although the survey forms used by NSTec in 2009 were not pre-marked UCNI, the completed forms contained no classification or unclassified control markings.<sup>20</sup>
6. The DOE investigation found that between 2009 and 2011, NSTec failed to obtain the requisite classification review for a total of 72 survey forms that were later determined to contain S/RD, which resulted in the inadequate protection and control of classified information.<sup>21</sup>

Collectively, these noncompliances constitute a Severity Level II violation.

Base Civil Penalty - \$55,000<sup>22</sup>

Proposed Civil Penalty (as adjusted for mitigation) - \$27,500

**B. Failure to process classified information on approved information systems and maintain cyber sanitization documentation**

NAP 70.4, Section A, *Classified Matter Protection and Control*, Paragraph 2., *Requirements*, subparagraph d., requires 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.”

---

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

<sup>20</sup> *Id.*

<sup>21</sup> *Id.*

<sup>22</sup> 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 is \$110,000. 74 Fed. Reg. 66033 (December 14, 2009). This rule adjusted DOE’s civil monetary penalties for inflation as mandated by the Debt Collection Improvement Act of 1996 (Act). Under the Act, the inflation adjustment for each applicable civil monetary penalty is determined by increasing the maximum civil penalty amount per violation by the cost-of-living adjustment (*i.e.*, for Severity Level II violations, the calculated increase is rounded to the nearest multiple of \$5,000 making the new adjusted Base Civil Penalty for Severity Level II violations \$55,000). This change will be applied to the proposed Base Civil Penalties for NSTec because the security event occurred after the effective date of the amendment to Part 824.

DOE Manual 205.1-5, Chg. 2, Attachment 1, Contractor Requirements Document, requires that “[r]egardless of the performer of the work, the contractor is responsible for implementing and complying with the requirements of . . . the applicable Senior DOE Management Program Cyber Security Plan (PCSP).”

DOE Manual 205.1-6, Chg. 2, Attachment 1, Contractor Requirements Document, requires that “[r]egardless of the performer of the work, the contractor is responsible for implementing and complying with the requirements of . . . the applicable Senior DOE Management Program Cyber Security Plan (PCSP).”

NAP 14.1-C, Chapter I, *NNSA PCSP Overview*, Paragraph 1., *Introduction*, states that “[t]he requirements of the NNSA PCSP, as detailed in this NAP, apply to any information system or network that is used to collect, create, process, transmit, store, or disseminate information for the NNSA. The NNSA PCSP implements National and Departmental cyber security policies.” Paragraph 5., *Certification And Accreditation*, states that “[t]he NNSA PCSP implements the National and Departmental requirements for the C&A of all information systems . . . . Each information system must receive an accreditation, *i.e.*, approval to operate (ATO) or an interim approval to operate (IATO), before beginning operational activities.”

In addition, Chapter XVI, *Clearing, Purging and Destroying Media*, Paragraph 1., *Introduction*, subparagraph c., states that this chapter establishes “[i]nstructions for sanitizing storage media that has become contaminated with classified or unclassified sensitive information.” Paragraph 2., *Criteria and Processes*, subparagraph f., *Special Circumstances*, (2) *Purging Partially Contaminated Storage Media*, states that “[a]reas of non-removable and removable storage media partially contaminated with an information type of a higher confidentiality impact or more restrictive Information Group may be purged . . . .” (d) States that “[q]uality controls are to be documented and deployed for review of overwrite process results and verification that all the contaminating information was completely overwritten.” (f) establishes the following criteria for records to be maintained, as a minimum:

- (1) Storage media unique identifiers, such as serial number, make, and model.
- (2) Contaminating Information Group.
- (3) Purpose of purging.
- (4) A statement that the storage media no longer contains the Information Group.
- (5) The procedure used.
- (6) The date, printed name, and signature of the certifying individual.

Contrary to these requirements, based on the following facts, NSTec processed classified information on information systems that were not certified or accredited to operate. In addition, NSTec failed to maintain the required media sanitization documentation.

1. NSTec radiological control technicians manually document radiological survey results on survey forms at the time measurements are taken, and then record the information electronically on unclassified information systems.<sup>23</sup> Although the radiological surveys were conducted for classified activities, the NSTec radiological control technicians did not have a derivative classifier review the survey forms before they processed the data on unclassified information systems.<sup>24</sup> As a result, 72 survey forms containing classified information were entered into information systems not certified or accredited for processing classified information.<sup>25</sup>
2. After NSTec discovered the security event in October 2011, it found that 51 material control and accountability (MC&A) forms associated with the 2009 classified activity included similar information as the survey forms and should have also been marked to reflect they contained S/RD information.<sup>26</sup> The MC&A forms had been reviewed by an NSTec derivative classifier/reviewing official, but were incorrectly determined to contain only UCNI information.<sup>27</sup> However, the DOE investigation confirmed that classified information derived from the MC&A forms was processed on information systems that were not certified and accredited for classified processing, and then transmitted by unauthorized means.<sup>28</sup>
3. The NSTec cyber security division was notified of this security issue (i.e., that 72 survey forms and 51 MC&A forms contained S/RD information) and informed of concerns that the survey forms and information derived from the MC&A forms had been processed on unclassified information systems, stored on unclassified shared drives, and transmitted by unauthorized means.<sup>29</sup> However, when NSTec cyber security personnel began to isolate and sanitize the contaminated information systems, they determined that the suspected classified files (i.e., approximately 200 documents) had already been deleted from one of the shared drives at the direction of the NSTec inquiry official.<sup>30</sup> As a result, NSTec cyber security personnel had to rely on a handwritten list of files reconstructed by the NSTec inquiry official in an attempt to appropriately perform the required sanitization.<sup>31</sup> The DOE investigation discovered that the cyber security division

---

<sup>23</sup> Investigation Report, *supra* note 2, at 5.

<sup>24</sup> *Id.*

<sup>25</sup> *Id.*

<sup>26</sup> *Id.* at 3.

<sup>27</sup> *Id.*

<sup>28</sup> *Id.* at 5.

<sup>29</sup> *Id.*

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*



failed to maintain the requisite documentation of its sanitization efforts and thus could not verify whether the handwritten list comprised all of the deleted classified files.<sup>32</sup>

4. NSTec cyber security personnel performed a follow-up scan to ensure all suspected classified files related to this security event had been appropriately removed.<sup>33</sup> The follow-up scan identified 243 suspected classified files many of which had previously been removed by NSTec cyber security personnel from the shared drive during its initial sanitization efforts.<sup>34</sup> NSTec cyber security personnel reported this anomaly to the NSTec inquiry official.<sup>35</sup> The NSTec inquiry official had the suspected files reviewed by a derivative classifier, who confirmed that most of the 243 files did, in fact, contain S/RD.<sup>36</sup> Later, when NSTec cyber security personnel proceeded to sanitize the affected shared drive, they found once again that the suspected classified files had been deleted and were unable to determine who placed the files on the shared drive or who deleted them.<sup>37</sup> Although NSTec cyber security personnel were able to use file notes to reconstruct NSTec's response and timeline of activities for this security issue, the DOE investigation determined that NSTec cyber security personnel failed to maintain the process, sanitization, and quality control documentation as required.<sup>38</sup>

Collectively, these noncompliances constitute a Severity Level II violation.

Base Civil Penalty - \$55,000

Proposed Civil Penalty (as adjusted for mitigation) - \$27,500

### C. Failure to conduct an adequate IOSC inquiry

DOE Manual 470.4-1, Chg. 2, Attachment 2, Contractor Requirements Document, Part 2, *Safeguards and Security Management*, Section N, *Incidents of Security Concern*, Paragraph 2., *Requirements*, subparagraph e., requires that “[i]nquiries must be conducted to establish the facts and circumstances surrounding an [IOSC].”

In addition, Section N, Chapter I, *Identification and Reporting Requirements*, Paragraph 2, *Incident Identification and Categorization*, requires that “DOE use a graded approach for identification and categorization of [IOSCs]. This approach provides a framework for the requirements of reporting timelines and the level of detail for inquiries into, and root cause analysis of, specific security incidents . . . .” Paragraph 3., *Reporting Requirements*, subparagraph g., *Closing Inquiries*, (1) requires that “IMI-1 and IMI-2 incidents are considered closed upon completion of the inquiry report. The inquiry report must be completed within 60 working days of

---

<sup>32</sup> *Id.* at 5-6.

<sup>33</sup> *Id.* at 6.

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

the incident categorization . . . .” Paragraph 6., *Conduct of Inquiries*, subparagraph b., establishes the following criteria for an IOSC inquiry:

(1) Data Collection.

- (a) Collect all data/information relevant to the incident, such as operations 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. (See Figure 2 for an example of a Chain-of-Custody Form.)

(2) Incident Reconstruction.

- (a) Reconstruct the [IOSC] 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. 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:

- (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, the NSTec inquiry was not timely, accurate, or thorough because it was not conducted in accordance with the established criteria for an IOSC, as described above.<sup>39</sup>

1. NSTec implements a graded approach in response to an IOSC based on the Impact Measurement Index (IMI) categorization.<sup>40</sup> IMI-1 and IMI-2 security incidents are given a higher priority and require completion of a Safeguards and Security Information Management System (SSIMS) incident inquiry report within 60 days from the date of categorization, a more rigorous causal/root cause analysis, and an extent-of-condition review.<sup>41</sup> Although NSTec categorized the subject incident as an IMI-2, the NSTec inquiry took nearly six months to complete.<sup>42</sup> The NSTec inquiry also lacked sufficient depth to identify all of the facts and circumstances surrounding this significant security event.<sup>43</sup>
2. The DOE investigation found that inappropriate actions resulting from NSTec inquiry efforts and incident reconstruction delayed completion of the NSTec inquiry and negatively impacted its overall accuracy and thoroughness.<sup>44</sup> These actions included deleting suspected classified files from unclassified information systems and shared drives before notifying the NSTec cyber security division; permitting uncleared personnel to retrieve archived boxes containing suspected classified information; and directing an individual not authorized as a derivative classifier/reviewing official to identify potentially classified files based on verbal guidance.<sup>45</sup>
3. In addition, the DOE investigation discovered that NSTec failed to conduct any further inquiry upon discovering the additional 243 classified files on an unclassified shared drive after the cyber security division completed the initial scan and sanitization of contaminated files.<sup>46</sup> Without such an inquiry, NSTec was unable to determine by whom, by what means, and when the classified files were placed on the unclassified shared drive and who was responsible for deleting them before the required sanitization process began.<sup>47</sup>
4. Although most of the subject classified documents resulted from a classified activity in 2009 (before the development of the pre-marked UCNI survey form), the NSTec inquiry mainly focused on identifying who directed the development and use of the pre-marked UCNI survey form.<sup>48</sup> The NSTec inquiry did not address specific work control processes and standard operating procedures for radiological surveys

---

<sup>39</sup> NSTec completed an NSTec Final Inquiry Report on March 15, 2012; DOE received the report on August 7, 2012.

<sup>40</sup> Investigation report, *supra* note 2, at 7.

<sup>41</sup> *Id.*

<sup>42</sup> *Id.*

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

<sup>46</sup> *Id.*

<sup>47</sup> *Id.*

<sup>48</sup> *Id.* at 7-8.

involving classified subject areas to ensure requirements for classification reviews are clearly delineated and understood.<sup>49</sup> Furthermore, the DOE investigation determined that the NSTec inquiry causal analysis and resulting corrective actions focused primarily on human performance and supervisory methods, and failed to include and address shortcomings associated with work control processes and procedures.<sup>50</sup>

Collectively, these noncompliances constitute a Severity Level II violation.

Base Civil Penalty - \$55,000

Proposed Civil Penalty (as adjusted for mitigation) - \$27,500

#### **D. Failure to protect and control classified information**

NAP 70.4, Chg. 1, Section A, *Classified Matter Protection and Control*, Paragraph 2., *Requirements*, subparagraph a., requires that “[c]lassified matter that is generated, received, transmitted, used, stored, reproduced . . . or destroyed must be protected and controlled commensurate with classification level, category (if RD or FRD [Formerly Restricted Data]), and caveats (if applicable) . . . .” Subparagraph b. requires that “[a]ccess to classified matter must be limited to persons who possess appropriate access authorization . . . and who have a need-to-know . . . for the performance of official duties.” Subparagraph c. states that “[c]lassified matter must be stored in an authorized Property Protection Area in a General Services Administration-approved security container, closed area, Limited Area, Exclusion Area, Protected Area, or MAA [Material Access Area].” Subparagraph f. states that “[b]uildings and rooms containing classified matter must be configured with security measures that prevent unauthorized persons from gaining access to classified matter; specifically, security measures that prevent unauthorized physical, visual, and aural access . . . .”

Contrary to these requirements, based on the following facts, NSTec failed to provide the necessary protection and establish the required controls for classified information.

1. As a result of NSTec’s failure to obtain the required classification review for newly generated documents in a classified subject area, a total of 123 forms (i.e., 72 survey forms and 51 MC&A forms) containing classified information were not marked, protected, or controlled as required.<sup>51</sup> Some of the survey forms and all of the MC&A forms were maintained in a facility authorized for the storage of classified information, but the forms were not appropriately marked or appropriately controlled.<sup>52</sup>
2. In 2011, the NSTec radiological control records consigner prepared the calendar year 2009 survey forms for archiving.<sup>53</sup> Among these holdings were 40 survey forms that

---

<sup>49</sup> *Id.* at 8.

<sup>50</sup> *Id.*

<sup>51</sup> *Id.* at 4.

<sup>52</sup> *Id.*

<sup>53</sup> *Id.*

were later determined to contain S/RD.<sup>54</sup> The NSTec radiological control records consigner does not possess a security clearance and therefore does not have authorized access to classified information.<sup>55</sup> Similarly, the offsite document storage facility personnel do not possess security clearances but had access to the archive boxes containing the classified survey forms.<sup>56</sup> The archive boxes (cardboard boxes sealed with packing tape) do not meet the requirements for packaging classified materials for transport, and the classified information was not stored by approved means.<sup>57</sup> In addition, the offsite document storage facility lacked the requisite facility approval and physical protection measures required by DOE to deter and detect unauthorized access.<sup>58</sup>

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

## II. Assessment of Civil Penalties

The significance of a security breach is a primary factor in NNSA's determination of an appropriate civil penalty. NNSA proposes the assessment of civil penalties for the violations identified in this PNOV because of NSTec's failure to identify classified information and provide appropriate protection and control to prevent unauthorized disclosure. Furthermore, NSTec could have prevented the additional potential security breaches by performing an adequate inquiry and maintaining the required supporting documentation on the cyber security sanitization process.

### A. Severity of the Violations

Both the NSTec inquiry and the DOE investigation concluded that a compromise of classified information could not be ruled out, and that unauthorized individuals had access to S/RD information in hard copy and electronic forms. The subject incident resulted from the failure to ensure the required classification review of information generated in a classified subject area. In addition, contrary to the advice given by the classification officer, NSTec used pre-marked survey forms that incorrectly identified the survey information as UCNI and created a false assumption that the information had been appropriately reviewed by an NSTec derivative classifier/reviewing official. This erroneous assumption significantly reduced the likelihood that anyone would question the classification of the information contained on the survey forms.

Furthermore, the circumstances surrounding this subject security incident involved forms generated in 2009 as well as in 2011. In total, 123 documents containing S/RD information were inappropriately marked, protected and controlled.

---

<sup>54</sup> *Id.*

<sup>55</sup> *Id.*

<sup>56</sup> *Id.*

<sup>57</sup> *Id.*

<sup>58</sup> *Id.*

In addition, the survey forms containing S/RD information were generated on unclassified information systems and stored on an unclassified shared drive. Classified information was also derived from the 51 inappropriately marked MC&A forms from 2009, which were transmitted by unauthorized means.

The DOE investigation determined that the NSTec inquiry was not timely, accurate, or thorough. The security event was appropriately categorized as an IMI-2, yet NSTec took nearly six months to complete the inquiry. Based on the narrow focus in determining the origin of the pre-marked UCNI survey form, the NSTec inquiry lacked sufficient depth to accurately and completely identify all the facts and circumstances associated with this security event. The effectiveness of the NSTec cyber security division's response was hindered by suspected classified files being deleted before NSTec cyber security personnel could appropriately isolate and sanitize contaminated information systems. Furthermore, NSTec cyber security personnel failed to maintain the process, sanitization, and quality control documentation as required.

## B. Mitigation of Penalties

NNSA provides strong incentives, through opportunity for mitigation, for contractors to self-identify and promptly report security noncompliances before a more significant event or consequence arises. The NSTec security program weaknesses identified by DOE should have been identified by NSTec before being revealed by this security event. Classified information was introduced into unauthorized information systems, transmitted by unauthorized means, and stored at unapproved locations.<sup>59</sup> NSTec became aware of a self-disclosing event and promptly reported it in SSIMS; that is commendable. However, in some cases, the noncompliant conditions existed for an extended period of time.<sup>60</sup> Consequently, NNSA finds that no mitigation for self-identification and reporting can be granted under 10 CFR 824, App. A.

Another mitigating factor considered by NNSA is the timeliness and effectiveness of contractor corrective actions. Upon discovery of the subject security event, NSTec took immediate corrective actions to locate all hard copies of the survey forms and determine whether other documentation could have been generated using information from these survey forms (e.g., electronic files and MC&A forms).<sup>61</sup> Nonetheless, the immediate corrective actions were mainly focused on management and human performance issues rather than the apparent weaknesses in NSTec work control processes and procedures.<sup>62</sup> However, in February 2014, DOE conducted a Security Enforcement Regulatory Assistance Review of the classified information security program managed by NSTec at NNSS. The review determined that the overall safeguards and security program is improving and NSTec leadership is committed to

---

<sup>59</sup> *Id.* at 8.

<sup>60</sup> *Id.* at 9.

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*

addressing past noncompliant conditions and enhancing its security performance. NSTec has successfully established a foundation for its classified information security program through recent efforts to develop and revise safeguards and security processes and procedures. In addition, this review identified attributes that point to NSTec's ability to continue its efforts to improve and sustain effective security performance and provide increased confidence in the long-term effectiveness of corrective actions taken for this security event. As a result, NNSA finds that mitigation is fully warranted for corrective actions.

### C. Civil Penalties

NNSA concludes that a penalty is fully warranted in this case. While civil penalties assessed under 10 C.F.R. Part 824 should not be unduly confiscatory, they should nonetheless 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.

In light of these considerations, NNSA proposes the imposition of a civil penalty of \$220,000 for the four Severity Level II violations, less 50 percent mitigation for corrective actions, resulting in a total proposed civil penalty of \$110,000.

### III. Opportunity to Reply

Pursuant to 10 C.F.R. § 824.6(a)(4), NSTec may submit a written reply to this PNOV within 30 calendar days of receipt of the PNOV. NSTec 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 NSTec 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.

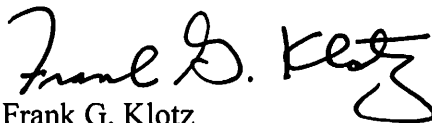
If NSTec chooses not to contest the violations set forth in this PNOV and the proposed remedy, then the reply should state that NSTec waives the right to contest any aspect of this PNOV and the proposed remedy. In such case, the total proposed civil penalty of \$110,000 must be remitted within 30 calendar 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 Nevada Field Office.

Pursuant to 10 C.F.R. § 824.6(c), if NSTec fails to submit a written reply within 30 calendar days of receipt of this PNOV, NSTec 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 <sup>26<sup>th</sup></sup> day of *sep* 2014