Report No. DODIG-2023-037

~~CUI~~

INSPECTOR GENERAL

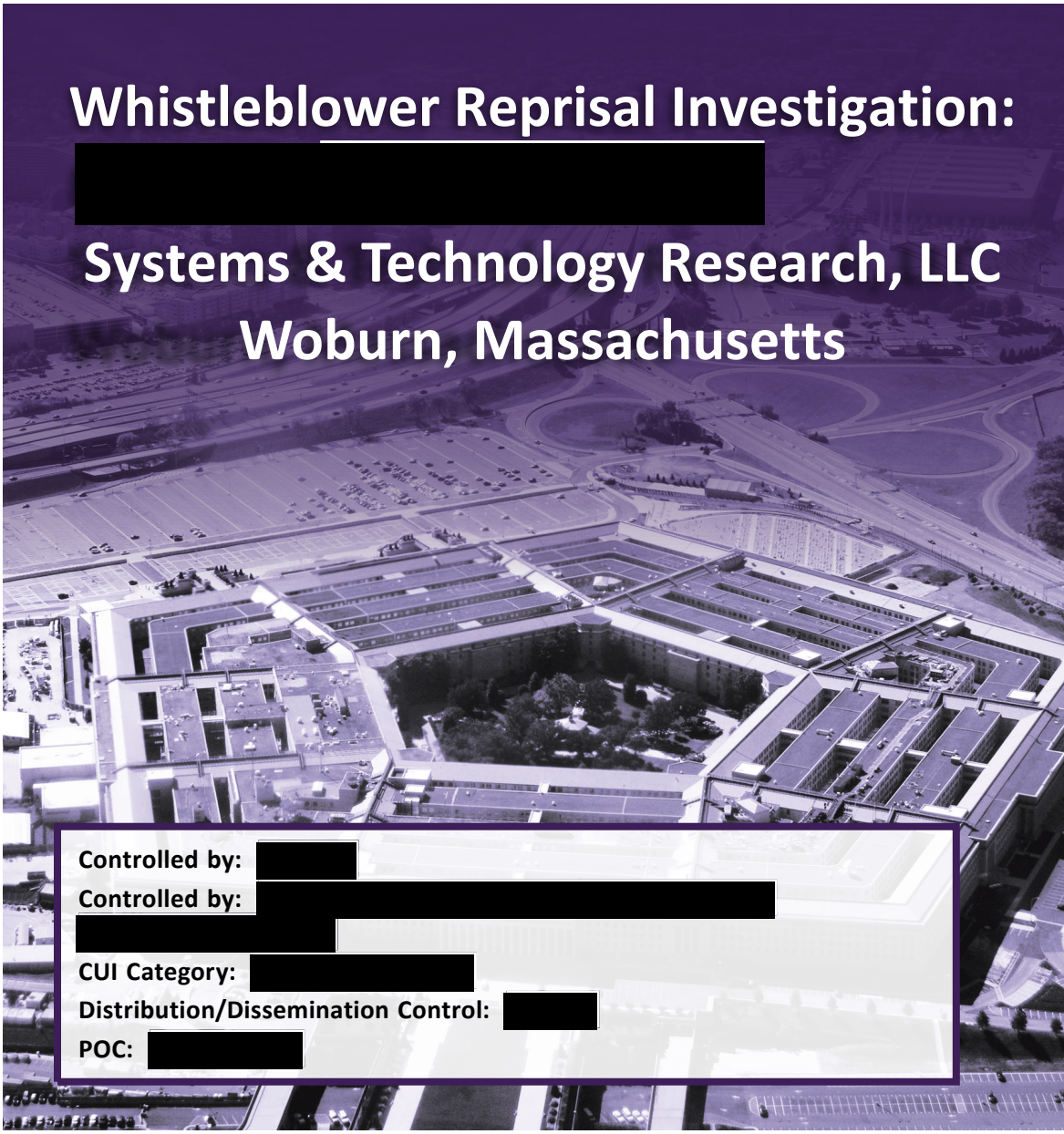
U.S. Department of Defense

DECEMBER 13, 2022

Whistleblower Reprisal Investigation:

[redacted]

Systems & Technology Research, LLC
Woburn, Massachusetts



Controlled by: [redacted]
Controlled by: [redacted]
CUI Category: [redacted]
Distribution/Dissemination Control: [redacted]
POC: [redacted]

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~CUI~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Table of Contents


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

WHISTLEBLOWER REPRISAL INVESTIGATION: [redacted]

SYSTEMS & TECHNOLOGY RESEARCH, LLC WOBURN, MASSACHUSETTS

Executive Summary

We conducted this investigation in response to a reprisal complaint alleging that Systems & Technology Research, LLC (STR), Woburn, Massachusetts, moved the Complainant's office location and discharged him in reprisal for making protected disclosures concerning security violations.

[redacted] Security Officer, STR (the Complainant), made eight protected disclosures from October 2019 through November 11, 2020, comprising:

- two to the Vice President of Business Operations,
- one to the Senior Vice President of Operations,
- one to the Director of Security,
- one to the DoD Hotline,
- one to the Security Manager,
- one to an industrial security representative from the Defense Counterintelligence and Security Agency (DCSA), and
- one to both the Senior Vice President and Deputy Vice President of Business Operations; the latter was also the Acting Human Resources (HR) Lead.

The company had direct knowledge of seven of the disclosures before relocating the Complainant's office. The company took steps to discharge the Complainant before the eighth disclosure; however, it did not carry out the discharge until after the eighth disclosure.

Based on knowledge and timing, the Complainant's protected disclosures were a contributing factor in STR's decision to relocate the Complainant's office and discharge him. Lacking clear and convincing evidence establishing that STR would have relocated the Complainant's office and discharged him absent his protected disclosures, we determined that STR took those actions in reprisal for the Complainant's protected disclosures.

We provided STR the opportunity to comment on the preliminary report of investigation through a tentative conclusions letter we sent to STR on September 21, 2022. We received STR's response on October 5, 2022. STR disagreed with our conclusions and requested

that we revise our report and conclusion to be consistent with its response. After carefully considering the response, we amended various sections of the report but did not alter our original conclusion.[1]

We recommend that the Secretary of the Navy direct Navy officials to:

- consider appropriate action against STR for reprising against the Complainant; and
- order STR to award the Complainant compensatory damages (including back pay), employment benefits, and other terms and conditions of employment that the Complainant would have received had he not been reprised against.

[1] While we have included what we believe is a reasonable synopsis of STR's responses, we recognize that any attempt to summarize risks oversimplification and omission. We incorporated its comments where appropriate throughout this report and provided a copy of its full responses to the Secretary of the Navy, along with this report.

Background

STR Contract and Location

STR hired the Complainant in June 2017 to work as a contractor program security officer (security officer) in its Woburn, Massachusetts office. The Complainant's work focused on multiple Special Access Programs (SAP). He worked across several contracts for Government customers within the DoD. One of the Complainant's major Government customers was the Defense Advanced Research Project Agency (DARPA). The Complainant also performed work for Government customers in the Intelligence Community. STR was the prime contractor under contract N65236-19-C-8010, a U.S. Navy contract issued on behalf of DARPA. The DCSA granted a facility security clearance to STR, where the Complainant worked. This authorized STR to operate classified information systems and safeguard classified information. The Complainant's disclosures of security violations related directly to DARPA programs.

The Complainant

The Complainant had over 20 years of experience working as a security officer. He worked at STR from June 5, 2017, until STR discharged him on November 16, 2020. The Complainant supported multiple SAPs and was responsible for:

- the management, direction, administration, and development of security programs and procedures for those assigned programs that have contractually imposed security requirements in excess of normal operating requirements;
- the interface with Government agencies regarding assigned program security matters and requirements; and
- the Prior Approval Request process, inspections preparation, visit requests, security briefings, refreshers and debriefings, access rosters, classified mail, management systems access, and other duties as assigned.

The Complainant's direct supervisor changed three times during his tenure at STR. His first supervisor was Security Manager [redacted]. [redacted] left the company around July or August 2020, and [redacted] became the new Security Manager. Around the August or September 2020 period, Security Officer [redacted] became the Security Officer Team Lead, a new supervisory position. On September 29, 2020, [redacted] asked to be removed from the team lead position, and [redacted] became the Complainant's supervisor again. Management officials involved in the decision to discharge the Complainant were [redacted]; [redacted], Senior Vice President (VP) of Business Operations; [redacted], Deputy VP of Business Operations and Acting HR Lead; and [redacted], Director of Security. Management officials involved in the decision to relocate the Complainant's office were [redacted] and [redacted]. [redacted] held the additional role of Acting HR Lead from April 2020 to March 2021.

Key Laws, Regulations, and Policies Pertaining to the Complainant's Disclosures

Safeguarding Classified Information: Overarching DoD Regulation

DoD 5220.22-M, "National Industrial Security Program: Operating Manual," February 28, 2006 (Incorporating Change 2, May 18, 2016) (NISPOM) is "issued in accordance with the National Industrial Security Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information."[2] Executive Order 12829, "National Industrial Security Program," January 6, 1993, established the NISP for the protection of classified information. The NISP applies to the entire DoD and to all cleared contractor facilities located within the United States.[3] The DCSA administers the NISP on behalf of the DoD.

Insider Threats

According to the NISPOM, section 1-300, "Contractors are required to report certain events that: impact the status of the facility clearance; impact the status of an employee's personnel security clearance; may indicate the employee poses an insider threat; affect proper safeguarding of classified information; or that indicate classified information has been lost or compromised." Section 1-300.a further provides that "[c]ontractors shall establish such internal procedures as are necessary to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the [Facility Security Officer], the Federal Bureau of Investigation (FBI), or other Federal authorities as required by this manual, the terms of a classified contract, and U.S. law. Contractors shall provide complete information to enable the CSA [Cognizant Security Agency] to ascertain whether classified information is adequately protected. Contractors shall submit reports to the FBI and to their CSA as specified in this section."

Security Violations

DoD Manual 5205.07 Volume 1, "DoD Special Access Program (SAP) Security Manual: General Procedures," June 18, 2015 (Incorporating Change 2, Effective September 30, 2020) (SAP Volume 1), requires that "[a]ll security violations will be reported immediately, to the extent possible, and no later than 24 hours of discovery, to the [Program Security Officer], through the procedures described in this enclosure."[4]

---

[2] DoD 5220.22-M, section 1-100.a, states, "The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information." In November 2021, the NISPOM was incorporated into Title 32 Code of Federal Regulations part 117 (2022).

[3] DoD 5220.22-M, section 1-102.a.

[4] The previous version of DoD Manual 5205.07 Volume 1 in effect at the time of some of the protected disclosures also provided the same guidance.

DoD Manual 5205.07 Volume 2, "DoD Special Access Program (SAP) Security Manual: Personnel Security," November 24, 2015 (Incorporating Change 2, Effective October 30, 2020) (SAP Volume 2), requires all individuals with SAP access to report behavior such as alcohol abuse or criminal conduct to the Program Security Officer, Government Special Access Program Security Officer, or Contractor Program Security Officer. It also requires the immediate reporting of all security infractions and violations to the Program Security Officer, Government Special Access Program Security Officer, or Contractor Program Security Officer.[5]

The NISPOM, section 1-302.a, requires contractors to report adverse information coming to their attention concerning any of their cleared employees. The termination of an employee does not obviate the reporting requirement. The NISPOM defines adverse information as "[a]ny information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, that his or her access to classified information clearly may not be in the interest of national security, or that the individual constitutes an insider threat."

The NISPOM, section 1-303, requires contractors to report the loss, compromise, or suspected compromise of classified information, foreign or domestic, to the DCSA.

The NISPOM, section 4-102, states derivative classification responsibilities for contractors, which include the requirement to observe and respect original classification decisions and carry forward pertinent markings to newly created documents.

COVID-19 Protocols

The World Health Organization declared the Coronavirus Disease–2019 (COVID-19) outbreak a public health emergency of international concern on January 31, 2020. The World Health Organization declared COVID-19 to be a pandemic on March 11, 2020, and 2 days later, the President declared a nationwide emergency. Various states began to shut down on March 15, 2020, to prevent the spread of COVID-19.[6]

The STR "Company COVID-19 Travel Policy in Effect During November 2020" required employees who traveled outside the state or commuting area to obtain a negative FDA EUA-approved molecular (PCR) COVID-19 test no earlier than 72 hours after their date of return.[7] At the time, the Governor of Massachusetts had issued a COVID-19 order that required a 14-day quarantine for people entering the state unless they were traveling from a designated "lower-risk State." Employees were released from quarantine if they obtained a negative COVID-19 test after arriving in Massachusetts.

[5] The previous version of DoD Manual 5205.07 Volume 2 in effect at the time of some of the protected disclosures also provided the same guidance.

[6] Centers for Disease Control and Prevention, "CDC Museum COVID-19 Timeline," January 5, 2022.

[7] FDA EUA-approved is Federal Drug Administration Emergency Use Authorization-approved.

Scope

This investigation covered the period from October 2019, the date of the Complainant's first protected disclosure, through November 16, 2020, the date of the Complainant's discharge. We interviewed the Complainant, STR management officials, and relevant witnesses. We reviewed documentary evidence regarding departmental and organizational policies, written communications, e-mails, and qualifying records.

The DoD Office of Inspector General employs a two-stage process in conducting whistleblower reprisal investigations. The first stage focuses on the alleged protected disclosures, qualifying actions, and the subject's knowledge of the protected disclosures. The second stage focuses on whether or not the subject would have discharged, demoted, or otherwise discriminated against the employee absent the protected disclosures.

To progress to the second stage of the analysis, sufficient evidence, based on proof by a preponderance of the evidence, must be available to make three findings.

1. The complainant made a protected disclosure.
2. The complainant received a qualifying action.
3. The protected disclosure was a contributing factor in the qualifying action.

If a preponderance of the evidence supports these three findings, the analysis will proceed to the second stage. In the second stage, we weigh together three factors.

1. The strength of the evidence in support of the qualifying action
2. The existence and strength of any motive to retaliate on the part of the officials who were involved in the decision
3. Any evidence that the subject took similar actions against similarly situated employees who did not make protected disclosures

Unless clear and convincing evidence establishes that STR would have discharged, demoted, or otherwise discriminated against the Complainant absent his protected disclosures, a preponderance of the evidence establishes that the actions were taken in reprisal.

Whistleblower Protection for Contractor Employees

The DoD Office of Inspector General conducts whistleblower reprisal investigations involving employees of DoD contractors, subcontractors, grantees, subgrantees, and personal services contractors under section 2409, title 10, United States Code (10 U.S.C. § 2409), "Contractor Employees: Protection from Reprisal for Disclosure of Certain Information," as amended by Public Law 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021," section 1863(b), "Contractor Workforce," January 1, 2021, as amended, as implemented by Defense Federal Acquisition Regulation Supplement Subpart 203.9, "Whistleblower Protections for Contractor Employees."[8]

[8] Congress renumbered 10 U.S.C. § 2409 to 10 U.S.C. § 4701 effective January 1, 2022, pursuant to sections 1801(d)(1) and 1863(b) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law 116-283. Because the DoD Office of Inspector General received the complaint in this case before the effective date of the renumbering, references to the governing statute in this report reflect the statute in effect at the time, 10 U.S.C. § 2409.

Findings

Background Event – DARPA Account-Sharing Incident

The Complainant made two protected disclosures in October 2019. The catalyst for the subsequent six disclosures was the notification by an STR Information System Security Manager to STR Security Officer [redacted] on August 13, 2020, that several STR employees shared their DARPA SAP classified user accounts as recently as the night before.

Per SAP Volume 1, the account-sharing incident should have been reported to DARPA within 24 hours; however, STR's management directed Security Officer [redacted] to wait, investigate, and determine if a notification was necessary. After several days, [redacted] decided he was well beyond the reporting requirement, and he needed to notify DARPA. Therefore, on August 18, 2020, he wrote an official STR incident report, which included the detail that STR management told him to delay notifying DARPA. [redacted] sent it to two DARPA security officials, [redacted] and [redacted], the next day. In her reply to STR, [redacted] requested the names of those who instructed [redacted] to delay reporting the incident to DARPA.

On August 26, 2020, Security Officer [redacted], team lead, advised Security Director [redacted] of DARPA's response. [redacted] then told STR Chief Executive Officer (CEO) [redacted] and other STR management, including the Head of Information Assurance, [redacted], that he believed the report Security Officer [redacted] submitted was not entirely accurate. Later the same day, Security Director [redacted] advised CEO [redacted] that he did an internal review and found that [redacted] thought he heard from either Information Assurance Lead [redacted] or Information System Security Manager [redacted] that [redacted] said to wait to report to DARPA until STR leadership was notified. [redacted] told CEO [redacted] he did not tell [redacted] or [redacted] to wait, and that [redacted] "sat on it and reported 6 days later."

However, documentary evidence contradicts what Security Director [redacted] told CEO [redacted] on August 26, 2020. On Friday, August 14, 2020, a day after the account-sharing incident, Security Officer [redacted] e-mailed Security Manager [redacted] and Information Assurance Lead [redacted] asking if Security Director [redacted] was aware that he intended to notify DARPA security officials about the incident. Approximately 28 minutes later, [redacted] e-mailed [redacted], asking him to confirm that they should delay notifying DARPA. [redacted] confirmed they should delay notifying DARPA and that [redacted] was aware of the situation. [redacted] then replied to all three, plus two others, stating that based on [redacted]'s e-mail, he would delay notifying DARPA until further instructed. That evening, [redacted] replied, "All, based on what I understand of the situation if we decide to report to the external customer lets [*sic*] be sure we've had a chance to notify leadership we're doing so. Have a good weekend." Five days later, [redacted] notified DARPA without STR leadership's instruction to do so.

After learning that Security Officer [redacted] notified DARPA about the incident and included in his report that he was instructed to delay reporting, [redacted] wrote Security Director [redacted] and Security Manager [redacted] on August 26, 2020, stating that he believed [redacted] made the statement in the report to DARPA about delayed reporting to place the blame elsewhere. [redacted] wrote, "The sad reality is that this sort of thing can strain relationships with customer [*sic*] and doesn't look good for all of STR Security." [redacted] replied, "I agree, I'm floored and I think I'm at my wit's end with [redacted]."

Security Manager [redacted] then rewrote Security Officer [redacted]'s original report and submitted a new report to DARPA Security Officer [redacted] on August 27, 2020. In the new report, STR removed references to an STR employee admitting to knowingly breaching the SAP user agreement and to [redacted] being directed to delay reporting. STR's new report blamed [redacted] and the other security officers for not notifying the DARPA I20 Security Team within the required 24 hours and stated that it was an oversight on the part of STR's Security Staff. STR reported that it addressed this incident by retraining its security officers on security incident reporting timelines.

Protected Disclosures

Section 2409, title 10, United States Code, as amended by Public Law 116-283, prohibits a DoD contractor, subcontractor, grantee, subgrantee, or personal services contractor from discharging, demoting, or otherwise discriminating against an employee in reprisal for disclosing, to an authorized recipient, information that the employee reasonably believes is evidence of:

- gross mismanagement of a DoD contract or grant;
- a gross waste of DoD funds;
- an abuse of authority relating to a DoD contract or grant;
- a violation of law, rule, or regulation related to a DoD contract (including the competition for or negotiation of a contract) or grant; or
- a substantial and specific danger to public health or safety.

Protected disclosures also include providing evidence of contractor or subcontractor misconduct in any judicial or administrative proceeding relating to waste, fraud, or abuse on a DoD contract or grant.

Authorized recipients of such information are:

- a Member of Congress or a representative of a committee of Congress;
- an Inspector General;
- the Government Accountability Office;

- an employee of the DoD responsible for contract oversight or management;
- an authorized official of the Department of Justice or other law enforcement agency;
- a court or grand jury; and
- a management official or other employee of the contractor or subcontractor who has the responsibility to investigate, discover, or address misconduct.

Overview of Alleged Protected Disclosures

A preponderance of the evidence established that the Complainant made eight disclosures, all of which were protected under 10 U.S.C. § 2409.

Disclosure 1: Report to Deputy VP [redacted] About Failure to Report Adverse Information

Around October 1, 2019, the Complainant reported to Deputy VP [redacted] that he believed Security Director [redacted] did not follow adverse information reporting requirements.

According to the Complainant, STR Senior Information Technology (IT) Systems Administrator [redacted] told him in October 2019 that Security Director [redacted] asked [redacted] to monitor the computer of Security Manager [redacted] who was the Security Manager and the Complainant's first supervisor until July or August 2020. [redacted] told us that [redacted] asked him and IT Systems Administrator [redacted] to monitor [redacted]'s computer to check for removal of proprietary STR data because [redacted] was concerned [redacted] might take STR data and methodologies to a new job.

Deputy VP [redacted] recalled the Complainant bringing this issue to her attention, but she said that [redacted] had already made her aware of Security Director [redacted]'s request. The Complainant believed that if [redacted] felt Security Manager [redacted] was removing data, then STR's Facilities Security Officer (FSO), [redacted], should be informed so he could determine if Government customers needed to be notified. In addition, the Complainant said that he felt he had an obligation as a security officer to report any wrongdoings or adverse information.[9]

Security Director [redacted] denied making a request to monitor Security Manager [redacted]'s computer. He alleged that he was making general inquiries into whether STR could protect itself from exfiltration of data, and someone misunderstood that he was talking about [redacted]. However, Deputy VP [redacted] confirmed to us that she talked to [redacted], and his request was specifically to look at [redacted]'s computer because he thought [redacted] was potentially an insider threat. [redacted]'s testimony is also inconsistent with statements given by multiple STR employees to the DCSA during its administrative inquiry

[9] Under DoD 5220.22-M, section 1-302.a, contractors are required to report adverse information regarding any of their cleared employees.

in September and October 2020. The inquiry focused on possible security violations at STR. The DCSA interviewed 13 people, including IT Systems Administrators [redacted] and [redacted]; [redacted], former STR Vice President; VP [redacted] and [redacted]. They all gave statements that [redacted] did request that [redacted]'s computer be monitored. Therefore, we found [redacted]'s testimony to be less credible than that of [redacted] or the Complainant.

A reasonable person with knowledge of the facts known to the Complainant would have believed that an employee suspected of stealing proprietary data should be reported to a facility security officer or the DCSA, as required by the NISPOM, sections 1-300.a and 1-302.a. A failure to report that employee could reasonably be seen as a violation of a regulation related to a DoD contract. Additionally, Deputy VP [redacted] is a management official of the contractor with the responsibility to investigate, discover, or address misconduct. Accordingly, she was an authorized recipient of such a disclosure. Therefore, the Complainant's October 2019 disclosure to [redacted] was protected under 10 U.S.C. § 2409.

Disclosure 2: Report to Security Director [redacted] About Failure to Report an Insider Threat

According to the Complainant, in mid-October 2019, Security Director [redacted] asked him if he told Deputy VP [redacted] about his request to have IT monitor Security Manager [redacted]'s computer. The Complainant said that he told [redacted] he notified [redacted], and [redacted] tried to convince him that [redacted] was an insider threat and that STR supported his actions to monitor [redacted]. The Complainant said that he then asked [redacted] what steps he had taken, and the Complainant advised [redacted] that he should have notified the DCSA and removed [redacted]'s classified accounts if he believed [redacted] was an insider threat. The Complainant told us that [redacted] told him he did not contact the DCSA or remove [redacted] from his classified account.

Security Director [redacted] denied the Complainant's version of events, telling us that he never asked the Complainant if the Complainant reported him to Deputy VP [redacted] However, we found [redacted]'s testimony less credible than the Complainant's, given [redacted]'s inconsistent statements regarding the request to monitor [redacted]'s computer. Moreover, [redacted] confirmed that the Complainant brought this issue to her attention, and she spoke to [redacted] about it.

A reasonable person with knowledge of the facts known to the Complainant would have believed that an employee suspected of being an insider threat is adverse information that must be reported to the DCSA. The NISPOM, section 1-302.a., requires contractors to report adverse information, which includes information that may indicate an employee poses an insider threat. Failing to make such a report could reasonably be interpreted as a violation of the NISPOM, which is a regulation related to a DoD contract. Additionally, as STR's Director

of Security, [redacted] was a management official of the contractor with the responsibility to investigate, discover, or address misconduct. Accordingly, he was an authorized recipient of such a disclosure. Therefore, the Complainant's October 2019 disclosure to [redacted] was protected under 10 U.S.C. § 2409.

Disclosure 3: Report to the DoD Hotline About Possible Security Violations

The Complainant filed a complaint with the DoD Hotline on August 21, 2020, alleging that STR was not following security reporting procedures, and specifically that:

- Security Director [redacted] directed STR employees not to clean up the spill of classified data on a non-classified laptop;
- Security Director [redacted] accused a manager of being an insider threat but did not notify the Government;
- an STR vice president falsified the time on a Standard Form 702, "Security Container Check Sheet," during an investigation;
- Security Director [redacted] told the Complainant that DD Form 254, "Contract Security Classification Specification," is just policy, not a law;
- a business unit lead cursed at an employee because he was told that classified documents could not be sent until they were marked properly;
- an STR employee was not flagged in the Joint Personnel Adjudication System after the employee sent classified information over the company's non-classified network; and
- the work environment had a toxic work culture in which employees were afraid to report security violations for fear of repercussions.[10]

A reasonable person with knowledge of the facts known to the Complainant would have believed that failure to report an insider threat was a violation of the NISPOM, section 1-300. This instruction requires that contractors report events that may indicate an employee is an insider threat. Likewise, a reasonable person could have believed that failure to clean a data spill was a violation of the NISPOM, section 1-303, requirement to report any loss or compromise of classified information. Additionally, a reasonable person could have believed that failure to report an employee falsifying the time on a Standard Form 702 and to flag that employee in the Joint Personnel Adjudication System was a failure to report adverse

[10] The purpose of Standard Form 702, "Security Container Check Sheet," is to provide a record of the names and times persons have opened, closed, and checked a particular container that holds classified information. The purpose of DD Form 254, "Contract Security Classification Specification," is to convey security requirements and classification guidance and provide handling procedures for classified materials received or generated on a classified contract. The Joint Personnel Adjudication System was the enterprise system for personnel security, suitability, and credentialing management for DoD military, civilian, and contractors. It was replaced by the Defense Information Security System on March 31, 2021.

information regarding a cleared employee as required by the NISPOM, section 1-302.a. Lastly, a reasonable person could believe that preparing to send classified documents that were not properly marked violated NISPOM, section 4-102, "Derivative Classification Responsibilities."

Additionally, the DoD Hotline is part of the DoD Office of Inspector General, an authorized recipient of such a disclosure. Therefore, the Complainant's August 21, 2020 disclosure to the DoD Hotline was protected under 10 U.S.C. § 2409.

Disclosure 4: Report to Deputy VP [redacted] About Security Director [redacted]'s Behavior and Security Violations

The Complainant e-mailed Deputy VP [redacted] and STR HR Representatives [redacted] and [redacted] about Security Director [redacted] on September 13, 2020. The e-mail covered 24 issues, many of which focused on [redacted]'s management style and character, including his abusive behavior, temperament, anger, and inappropriate language. The Complainant's other allegations included that [redacted] played a role in falsifying the account-sharing incident report to DARPA and omitted information in the revised security report and sent the revised report to DARPA without notifying the originator of the report.

A reasonable person with knowledge of the facts known to the Complainant would have believed that falsifying or omitting information from an official security incident report to DARPA, a Government agency, was a violation of the NISPOM, section 1-302.a. Additionally, Deputy VP [redacted] was a management official of the contractor who had the responsibility to investigate, discover, or address misconduct. Accordingly, she was an authorized recipient of such a disclosure. Therefore, the Complainant's September 13, 2020 disclosure to [redacted] was protected under 10 U.S.C. § 2409.

Disclosure 5: Report to VP [redacted] About Security Director [redacted]'s Behavior and Security Violations

The Complainant met with VP [redacted] on or around September 21, 2020, to discuss the allegations in his September 13, 2020 e-mail to Deputy VP [redacted] The Complainant and [redacted] discussed the DARPA account-sharing incident, the accusation regarding a failure to clean a data spill on a laptop, and other topics in the e-mail.

A reasonable person with knowledge of the facts known to the Complainant would have believed that falsifying and omitting information in a report to DARPA, a Government agency, was a violation of the NISPOM, section 1-302.a. Additionally, VP [redacted] was a management official of the contractor with the responsibility to investigate, discover, or address misconduct. Accordingly, he was an authorized recipient of such a disclosure. Therefore, the Complainant's September 21, 2020 disclosure to VP [redacted] was protected under 10 U.S.C. § 2409.

Disclosure 6: Report to the DCSA About Security Violations

The DCSA conducted an administrative inquiry from August 26, 2020, to January 11, 2021, into allegations that Security Director [redacted] directed improper cleanup of a classified data spill, failed to address reported security violations, and failed to report security violations and individual culpability to the U.S. Government. On September 30, 2020, DCSA Industrial Security Representatives (ISR) [redacted] and [redacted] interviewed the Complainant. The Complainant raised several concerns to them, including those from his September 13, 2020 e-mail disclosing [redacted]'s failure to clean up the spill of classified data on a non-classified laptop as well as [redacted]'s attempt to have Security Manager [redacted]'s computer monitored. They also discussed the alleged falsified report to DARPA.

A reasonable person with knowledge of the facts known to the Complainant would have believed that a failure to report an insider threat, failure to clean up a data spill, and submission of a false report to the Government were violations of the NISPOM, sections 1-300, 1-303, and 1-302.a, respectively. The Complainant provided evidence of contractor misconduct during an administrative proceeding related to fraud, waste, or abuse on a DoD contract. DCSA ISRs [redacted] and [redacted] were Government officials responsible for security oversight of the contract. Therefore, the Complainant's September 30, 2020 disclosure to [redacted] and [redacted] was protected under 10 U.S.C. § 2409.

Disclosure 7: Report to Deputy VP [redacted] and VP [redacted] About COVID-19 Safety Concerns

Security Manager [redacted] held a meeting with the security officers on September 10, 2020. [redacted] raised the topic of relocating people into different offices and indicated that the Complainant would be moved out of the classified security office into an office in an unclassified area. After the meeting, the Complainant called [redacted] and told him that he had COVID-19 exposure concerns about the office move [redacted]. The Complainant felt safe in the security office because it had a "Dutch door" that prevented people from freely walking into the area.[11] The Complainant also told [redacted] that moving would make it hard for him to perform his job because the security office contained all of his classified information, secure phones, secure networks, and security access.

Security Manager [redacted] told us that the Complainant became irate during the September 10, 2022 meeting with the CPSOs when [redacted] brought up the idea of moving people around, and after the meeting, he told the Complainant that his behavior was unprofessional. [redacted] said he was aware of the Complainant's health concerns, but he said that topic did not come up during his September 10, 2020 meeting with the Complainant as a reason for the Complainant

[11] A "Dutch door" is a single door that is divided in the middle, allowing the user to open the top portion while keeping the bottom portion closed.

not wanting to move. [redacted] said the conversation focused on the Complainant's concern that the move was the result of an oral complaint from a coworker. In addition, [redacted] told us that the move was delayed from September to October because there was some back and forth with the Complainant.

On October 21, 2020, Security Manager [redacted] sent an e-mail to all 10 of the security officers, stating they would be shuffling the security officers' and alternate security officers' office assignments. He wrote that it would help "increase collaboration between [security officers] and [alternates]." Of the 10 employees identified in the e-mail, only 3 were to change offices. The Complainant was being removed from the Area 1 Security Office where he sat with Security Officers [redacted] and [redacted] Two alternate security officers were being moved into the Area 1 Security Office where the Complainant sat.

On the same day [redacted] sent the e-mail to the security officers, the Complainant forwarded the new seat assignment to Deputy VP [redacted] and VP [redacted] and requested a meeting. He informed [redacted] and [redacted] in the e-mail that moving was not in his best interests, for health or work, because he [redacted] and at a higher risk to catch COVID-19. In addition, the Complainant wrote that he spoke twice with [redacted] regarding his medical concerns related to moving offices, but he had not heard back from [redacted], and he felt that STR was moving him with no regard for his [redacted] concerns. The Complainant advised VPs [redacted] and [redacted] that he did not understand why Security Director [redacted] a COVID-19 Policy Committee member, would remove him from an area he felt safe working in throughout the COVID-19 pandemic. He also said that [redacted] and Security Manager [redacted] were aware of his [redacted] conditions, and all the equipment used or needed for his programs was in the Area 1 Security Office.

STR was aware of the Complainant's [redacted] conditions since June 2017, when he gave STR a note from his doctor to his former manager, Security Manager [redacted] shortly after he started working at STR. [redacted] told us that he received the note from the Complainant and either gave it to Deputy VP [redacted] directly or placed it on the STR HR shared drive.

VP [redacted] e-mailed the Complainant and Deputy VP [redacted] on October 23, 2020, stating that he understood the Complainant's medical concerns, but he wanted the alternates to sit next to the security officers so they could be mentored properly. He also wrote that he and [redacted] felt it was safer for the Complainant to have his own office away from coworkers and visitors. The Complainant responded that he did not feel it was safer, and he wanted to discuss the matter. The Complainant told us that he spoke with [redacted] and [redacted], but they moved him despite his health concerns. Conversely, STR informed us in its tentative conclusions letter response that it felt the Complainant's risk of COVID-19 exposure would be significantly reduced if STR provided him his own office rather than having him share the Area 1 Security Office with other CPSOs. STR said that the Complainant could control

his visits to the Area 1 Security Office and his interactions with other CPSOs as needed. The Complainant also told us that [redacted] and [redacted] agreed to provide a Dutch door on his new office to prevent people from freely walking in, but they never did. However, STR explained that at the Complainant's request, it submitted an installation order for the Dutch door on his new office in late October 2020, but STR did not receive the work agreement from the contractor until after STR discharged the Complainant, so the project was ultimately canceled.

A reasonable person with knowledge of the facts known to the Complainant during the height of the COVID-19 pandemic in 2020 would have believed that the Complainant's concerns regarding his potential exposure to COVID-19, as an [redacted] employee, posed a substantial and specific danger to public health.

Disclosure 8: Report to STR Management About Violations of COVID-19 Protocols

The Complainant e-mailed Security Manager [redacted] on November 11, 2020, and copied Security Director [redacted] VP [redacted] Deputy VP [redacted] and CEO [redacted] The Complainant disclosed that an employee in the Security Department returned to work from travel without following the STR COVID-19 policy. Specifically, the employee did not quarantine for 72 hours before getting a COVID-19 test. The Complainant also stated that the employee took a COVID-19 test within 24 hours of returning from travel, went to work the same day, and received authorization to do so. He stated that he was concerned because he and [redacted], and the employee at issue sat in close proximity to the Complainant.

The Complainant told us that the employee who was the subject of his e-mail was [redacted]. [redacted] told us that he obtained a negative COVID-19 test when he returned to Massachusetts from Florida, and he was unaware of the 3-day waiting requirement, so he went to work. Someone, possibly Security Manager [redacted] called [redacted] and told him to go home for 72 hours and then get the required PCR test. [redacted] did so and obtained a negative test result.

The STR "Company COVID-19 in Effect During November 2020" required employees who traveled outside the state or commuting area to obtain a negative PCR COVID-19 test no earlier than 72 hours after their date of return. At the time, the Governor of Massachusetts had issued a COVID-19 order that required a 14-day quarantine for people entering the state unless they were traveling from a designated "lower-risk State." The policy released employees from quarantine if they obtained a negative COVID-19 test after arriving in Massachusetts. Florida was not a "lower-risk State" at the time.

A reasonable person with knowledge of the facts as known to the Complainant would have believed that an employee who did not follow COVID-19 testing and quarantine protocols posed a substantial and specific danger to public health. Additionally, Security Manager [redacted] and the other e-mail recipients were management officials of the contractor who had responsibility to investigate, discover, or address misconduct. Accordingly, they were authorized recipients of such a disclosure. Therefore, the Complainant's November 11, 2020 disclosure to [redacted] and other STR management officials was protected under 10 U.S.C. § 2409.

Actions STR Took Against the Complainant

The 10 U.S.C. § 2409 statute prohibits discharge, demotion, or other discriminatory action with respect to any employee of a DoD contractor, subcontractor, grantee, subgrantee, or personal services contractor in reprisal for making a protected disclosure. Under 10 U.S.C. § 2409, an act of reprisal is prohibited even if it is undertaken at the request of a DoD official, unless the request takes the form of a nondiscretionary directive and is within the authority of the DoD official making the request.

The Complainant's Office Relocation

VP [redacted] with Deputy VP [redacted]'s consent, relocated the Complainant from the classified Area 1 Security Office to an unclassified solitary office on October 23, 2020. Relocating an employee's office away from required work equipment is an action that might well have dissuaded a reasonable employee from making a protected disclosure. Therefore, relocating the Complainant's office was a qualifying action under 10 U.S.C. § 2409.

The Complainant's Discharge

STR discharged the Complainant on November 16, 2020.

[redacted] told the Complainant that Deputy VP [redacted] wanted to see him in the conference room and suggested he take his backpack and personal belongings. The Complainant entered the conference room. [redacted] and [redacted] were in the room, and Security Manager [redacted] was on a video teleconference in the room. [redacted] advised the Complainant that he was discharged for poor performance. The Complainant asked what the issues were, and [redacted] said, "I think if you think back over to the past couple months, you know, you'll recall what." The Complainant responded that this was the first time he heard of anything, no one had pulled him aside, no one had counseled him, and he was shocked. [redacted] stated she was not there to talk about it, just to go over his benefits. [redacted] handed the Complainant a severance agreement, including a lump sum payment of [redacted] with a confidentiality and non-disparagement agreement. The Complainant did not sign the agreement.

A discharge is specifically identified as a qualifying action under 10 U.S.C. § 2409.

Qualifying Action

A preponderance of the evidence demonstrates that STR took two qualifying actions against the Complainant on October 23 and November 16, 2020.

Analysis

The evidence establishes that the Complainant's protected disclosures were factors in STR's decisions to relocate the Complainant's office and subsequently discharge him. Discussion of the factors weighed together follows the factor-by-factor analysis below, as appropriate.

Knowledge

A preponderance of the evidence establishes that it was more likely than not that STR knew of seven of the Complainant's protected disclosures before relocating his office and deciding to discharge him. STR began discussions about discharging the Complainant before his eighth disclosure, but it did not carry out the discharge until after the eighth disclosure.

Disclosure 1: Report to Deputy VP [redacted] About Failure to Report Adverse Information

Deputy VP [redacted] knew of the Complainant's early October 1, 2019 disclosure about Security Director [redacted] not following adverse reporting requirements when [redacted] instructed STR employees to monitor Security Manager [redacted]'s computer. The Complainant made this disclosure directly to [redacted].

Disclosure 2: Report to Security Director [redacted] About Failure to Report an Insider Threat

The Complainant made this disclosure directly to Security Director [redacted] around mid-October 2019 when he was confronted by [redacted] about whether the Complainant reported him to Deputy VP [redacted] The Complainant discussed [redacted]'s belief that Security Manager [redacted] was an insider threat and informed him of the correct protocol to report it. Although [redacted] asserted that this disclosure did not happen, we found [redacted]'s testimony not credible because testimony and documentary evidence gathered by the DCSA during its inquiry into alleged security violations contradicted it.

Disclosure 3: Report to the DoD Hotline About Security Violations

The Complainant filed his complaint with the DoD Hotline on August 21, 2020. The DoD Hotline referred the allegations to the DCSA, which opened an inquiry into STR's security practices on August 26, 2020. The evidence showed that STR was not aware that the Complainant contacted the DoD Hotline, but STR perceived the Complainant as making a disclosure to the DCSA, which resulted in the DCSA's investigation into STR's security practices.

DCSA ISR [redacted] called STR [redacted] on September 28, 2020, and asked him questions about Security Director [redacted] and security incidents, including classified information on an unclassified system and the subsequent cleanup. [redacted] hypothesized that the DCSA's inquiry was related to the Complainant and Security Officers [redacted]'s and [redacted]'s "discontent" with [redacted]'s behavior.

[redacted] told us that after the DCSA notified him of its investigation, he discussed the investigation with VP [redacted] but [redacted] said that they did not discuss who might have been responsible. However, [redacted] acknowledged that there were office and hallway discussions that the DCSA inquiry was likely related to either the Complainant or Security Officers [redacted] or [redacted] and their discontent with Security Director [redacted]

[redacted], said that he heard from [redacted] that there were rumors the DCSA inquiry started because of a report that was written and submitted to DARPA by either the Complainant or Security Officer [redacted] or both, that STR subsequently changed. According to [redacted], shortly after the DCSA inquiry began, [redacted] asked [redacted] if he called the DoD Hotline, and [redacted] said he did not. Then [redacted] asked [redacted] if the Complainant called the DoD Hotline because [redacted] thought the Complainant had. [redacted] said he did not know who called.

The Complainant told us that he did not inform anyone he was contacting the DoD Hotline other than Security Officers [redacted] and [redacted] however, word began to spread around STR during the DCSA investigation that the Complainant was "the whistleblower." [redacted] told the Complainant that [redacted] said the Complainant was the whistleblower. [redacted] told the Complainant that people thought he was the whistleblower, but the Complainant told [redacted] he "did not call DCSA," which the Complainant said was his way out when people asked, because he did not call the DCSA—he contacted the DoD Hotline.

[redacted] told us that [redacted] asked him if he was the one who contacted the DCSA, and then [redacted] asked him if the Complainant did, but [redacted] said he had no idea. [redacted] then told [redacted] that [redacted] believed the Complainant contacted the DCSA.

[redacted] told us that [redacted] informed him that an employee made an allegation to the DCSA; they did not know who, but "we just all presumed it was [the Complainant]." [redacted] said that he asked the Complainant if he was the one who filed the complaint with the DCSA, but the Complainant told him he did not. [redacted] said that the fact that the DCSA was investigating STR spread around the office, and people started saying, "I bet you it was the Complainant." According to [redacted], the word around the office was that the Complainant probably made a complaint to the DCSA.

[redacted] told us that when discussing with STR's attorneys the potential of discharging the Complainant, STR was concerned about the timing of it, given that the Complainant had submitted a complaint, and they weighed the risk of security issues versus being sued. While discussing with us how STR handled the Complainant's previous report to HR about STR not wiping a computer clean when there was a data spill, [redacted] said that he dug into the issue, and STR came up with a technique to both wipe the computer clean and save the information. [redacted] said that the DCSA was aware of what STR did then, so the DCSA investigated it once, and again "once [the Complainant] reported that."

Finally, e-mail documentation shows that DCSA ISR [redacted] contacted [redacted] on Monday, September 28, 2020, and [redacted] spoke to VP [redacted] about it on Tuesday, September 29, 2020. On September 30, 2020, CEO [redacted] e-mailed several STR officials, including [redacted], and notified them that a DCSA investigation was underway "triggered by reports from STR staff about our Security group leadership, specifically [redacted]." The e-mail subject was "Whistleblower report to DCSA," and the e-mail stated that the inquiry centered around hostile workplace issues and security irregularities on Security Director [redacted]'s watch, including:

- the DARPA account-sharing incident not being properly reported,
- a data spill from 2019 that was not handled properly, and
- a VP falsifying the time on a Form 702 (secure facility open/close log).

CEO [redacted] also informed the STR recipients in the e-mail that STR was already aware of the hostile workplace issues and security irregularities because they were previously brought to STR's attention in complaints submitted to STR HR by Security Officer [redacted] and the Complainant on September 11 and 13, 2020, respectively. CEO [redacted] then e-mailed the STR recipients again and told them to keep this information close and not disseminate it further. CEO [redacted] wrote that STR already investigated "the items" that [redacted] and the Complainant brought up, so he was confident the company would get through this STR Security culture issue.

Security Officer [redacted]'s previous complaint to STR focused on STR's security culture and Security Director [redacted]'s leadership style, including his direction to delay reporting the DARPA account-sharing incident to the Government; the Complainant's previous complaint to STR specifically mentioned both the DARPA account-sharing incident and the data spill. The fact that two of the Complainant's security allegations that he previously reported internally to the company were now the focus of the DCSA investigation gives credence to the fact that STR perceived the Complainant as making protected disclosures to the DCSA. The fact that CEO [redacted] titled the subject of his e-mail to STR managers, "Whistleblower report to DCSA," shows that STR viewed the Complainant as a whistleblower.

Disclosure 4: Report to Deputy VP [redacted] About Security Director [redacted]'s Behavior and Security Violations

The Complainant made this disclosure directly to Deputy VP [redacted] in a document dated September 13, 2020. The Complainant told [redacted] he was concerned with Security Director [redacted]'s behavior, character, and potential security violations.

Disclosure 5: Report to VP [redacted] About Security Director [redacted]'s Behavior and Security Violations

The Complainant made this disclosure directly to VP [redacted] on or around September 21, 2020. The Complainant and [redacted] discussed the DARPA account-sharing incident, the accusation regarding a failure to clean a data spill on a laptop, and other topics.

Disclosure 6: Report to the DCSA About Security Violations

The Complainant told VP [redacted] and Security Manager [redacted] on September 30, 2020, that the DCSA contacted him and asked him multiple questions about STR and the security culture. He wrote that it seemed as if the DCSA had a copy of his September 13, 2020 complaint letter to Deputy VP [redacted] and HR. [redacted] was aware of what he believed to be the security incidents the DCSA was investigating because he provided them to CEO [redacted] for him to notify the STR Board of Directors. [redacted] was also aware of the contents of the Complainant's September 13, 2020 complaint because he investigated the allegations. Therefore, it is more likely than not that [redacted] knew what the Complainant spoke about to DCSA investigators.

Disclosure 7: Report to Deputy VP [redacted] and VP [redacted] About COVID-19 Safety Concerns

The Complainant made these disclosures directly to Deputy VP [redacted] and VP [redacted] The Complainant told them that moving offices would be detrimental to his health and work and that he felt safe in the Area 1 Security Office. He also said that he [redacted] and at a higher risk to contract COVID-19, and all his resources for work were in the Area 1 Security Office.

Disclosure 8: Report to STR Management About Violations of COVID-19 Protocols

The Complainant made this disclosure directly to Security Manager [redacted] Security Director [redacted] VP [redacted] Deputy VP [redacted] and CEO [redacted] The Complainant told them a coworker traveled out of state and did not properly quarantine per STR COVID-19 policy.

Timing of Personnel Actions

The Complainant attempted to resolve STR security violations internally and made protected disclosures directly to STR as far back as October 2019. However, it was only after he contacted an external authority, the DoD Hotline, regarding STR's potential security violations and alleged cover-up that STR began to take actions against the Complainant. Within approximately 3 weeks of learning of the DCSA investigation and perceiving the Complainant as a whistleblower who contacted the DCSA, STR relocated the Complainant from his office and discharged him.

STR's knowledge of the protected disclosures, along with the close timing between STR learning of the protected disclosures and STR's decisions to relocate the Complainant's office and discharge him, establishes that the Complainant's protected disclosures were contributing factors in the qualifying actions.

Strength of the Evidence

Stated Reasons for STR Relocating the Complainant's Office

STR asserted that it relocated the Complainant's office on October 23, 2020, to move alternate security officers near security officers to increase collaboration between the two groups. STR also stated that it believed that the private office was more conducive to protecting the Complainant from COVID-19 exposure, and it was more centrally located to all of the computer labs.

[redacted] told us that the majority of security officer work was unclassified and only a "finite" amount was classified, which meant the Complainant would infrequently need to return to the classified Area 1 Security Office. However, [redacted] also said that the Area 1 Security Office was "where a lot of action happened" and "where a lot of basic customer service issues came up … basic day-to-day customer service." [redacted] told us that the Complainant did not have to go back to the Area 1 Security Office because the Complainant could find unused computer terminals in other labs.

STR told us that it moved the Complainant out of the Area 1 Security Office because it had "significant concerns" about the Complainant's "problematic" influence on [redacted].

[redacted] told us that when he became the security manager, he had one-on-one meetings with each of the CPSOs. He said that four of the CPSOs expressed that they felt like they were not getting the training or the mentoring they needed, that the work environment was a "clubhouse" made up of the Complainant, [redacted], and [redacted], and the rest were left out. [redacted] said that he found it difficult to make any improvements or changes without it being a "big deal" with the CPSOs; the Complainant was his biggest obstacle, he was "obstinate at every turn," and he would not do anything to help the process. [redacted]

explained that the Complainant, [redacted], and [redacted] were stuck in their ways, did not want to change, and were not open to new ideas. Furthermore, [redacted] was a follower, and if the Complainant did not support an idea, [redacted] would not support the idea.

As a result, [redacted] said that he met with VP [redacted] Deputy VP [redacted] and Security Director [redacted] a couple of times in or around October 2020 to discuss how to handle the situation. [redacted] told us that he was in favor of letting the Complainant go, but he thought, without the Complainant there, that [redacted] might be "savable."

To give us an example of the Complainant's disruptive behavior, [redacted] explained how the Complainant caused "big drama" when another employee came back from a trip to Florida and violated COVID-19 policy by returning to the office after taking a rapid COVID-19 test instead of a PCR COVID-19 test. According to [redacted], the Complainant wrote a letter to the President of the company saying "he felt like his life was threatened" because of that employee coming into the office. [redacted] considered that drama because the Complainant "jumped three levels and went to the President of the company" when the only violation of policy was that the employee took the wrong test.

We note that [redacted] referenced the Complainant's November 11, 2020 protected disclosure in which the Complainant e-mailed Security Manager [redacted] and copied Security Director [redacted] VP [redacted] Deputy VP [redacted] and CEO [redacted] and reported that [redacted] violated COVID-19 protocols. As described above, [redacted] told us that he obtained a negative COVID-19 test when he returned to Massachusetts from Florida, but he went to work without quarantining for 3 days. Someone, possibly Security Manager [redacted] called [redacted] and told him to go home for 72 hours and then get the required PCR test.

Evidence Counter to STR's Stated Reasons for Office Relocation

The Complainant told us that the Area 1 Security Office contained three shared terminals. DARPA was the Complainant's main portfolio, and the Area 1 Security Office was the main access point for DARPA's classified network. One other terminal, in a different lab, offered limited access to DARPA programs. The Complainant told us that the other terminal was located in a conference room that was often booked for meetings, and, if someone was not cleared for the program being discussed in the room, he or she would not be able to work at the terminal during the meeting.

The Complainant and [redacted] also contradicted Security Director [redacted]'s assertion regarding the amount of classified work a security officer performs. The Complainant told us that 75 to 80 percent of his work was classified, and [redacted] told us that 70 percent of his work was classified.

The Complainant also believed that his risk of catching COVID-19 was higher in the new office, putting him [redacted], at risk. Finally, the Complainant told us that STR's collaboration explanation did not make sense because his assigned alternate security officer was moved into the Area 1 Security Office when he was moved out.

Stated Reasons for STR Discharging the Complainant

STR stated that it discharged the Complainant for poor performance that began in 2017, the first year of his employment. VP [redacted] told us that he was the one who pushed for the Complainant's discharge, and he made the final decision after consulting with CEO [redacted] He told us that it became clear over the course of the 6 months leading to the Complainant's discharge that there were problems with his performance that could not be corrected. He said that STR consulted with its attorney about the risk and timing in discharging the Complainant after he filed a complaint, but they felt it was best for STR and the Government. We asked [redacted] for an example of the Complainant not getting the job done in 2020. He told us, "I don't have specifics on that. I'd have to go back to the documentation."

VP [redacted] could not provide a date the actual discharge decision was made, but he said "late October" and referenced e-mails turned over to us. In an October 23, 2020 e-mail chain discussing an internal complaint about Security Officer [redacted] stated to Security Manager [redacted] "I'd add this to the file on [redacted]" and "What documentation do we have on [redacted]? How about [the Complainant]? Can you send me what you have?" The fact that [redacted] was attempting to gather derogatory documentation on the Complainant and [redacted] to support STR's decision to discharge both suggested that [redacted] made the decision in late October 2020.

VP [redacted] also told DCSA ISR [redacted] on October 26, 2020, that he received additional reports from Security Officers [redacted] and the Complainant that they were unhappy with management but that their reports did not involve security violations. [redacted] also stated that [redacted] was great, but the others had performance issues, and it seemed like political infighting.

On November 4, 2020, VP [redacted] told DCSA ISR [redacted] that STR would be "terminating" the Complainant and Security Officer [redacted]. [redacted] said the Complainant and [redacted]'s Government customers were unhappy with their performance. [redacted] also said that their former manager, Security Manager [redacted] did not manage them well.[12]

In support of its position that it discharged the Complainant for performance reasons, STR produced seven e-mails, one from 2017, four from 2018, one from 2019, and one from 2020.

[12] [redacted] resigned from STR [redacted].

October 31, 2017 E-Mail

[redacted], STR Vice President, notified Deputy VP [redacted] and CEO [redacted] in October 2017 that a Government customer Program Security Officer, [redacted], was frustrated with STR's transition from a previous security officer to the Complainant. The deficiencies cited delays in paperwork, significant hand-holding, and unfamiliarity with the Sensitive Compartmented Information (SCI) database, Scattered Castles. The Complainant had no experience with SCI, Scattered Castles, or Sensitive Compartmented Information Facility management when STR hired him in June 2017. However, the individual who was to train and mentor the Complainant resigned from STR in September 2017. This left the Complainant as the only security officer at STR's Woburn office at that time.

April 3, 2018 E-Mail

When STR was deciding between Security Officer [redacted] and another candidate for a security officer position in April 2018, Deputy VP [redacted] advised VP [redacted] and CEO [redacted] that the most qualified candidate was [redacted], but he previously worked for the Complainant and she did not want [redacted] to follow the Complainant's lead on execution style. [redacted] also wrote that [redacted], [redacted], and others were not impressed with the Complainant.

May 30, 2018 E-Mail

In May 2018, in response to [redacted], VP of STR IT at that time, [redacted], STR Program Manager, said she needed more time to provide [redacted] with a list of the Complainant's performance deficiencies. STR asserted that [redacted] requested the removal of the Complainant from her project, so [redacted] asked her for a list of the specific issues. [redacted] was unable to locate her response e-mail to [redacted] that listed any specific issues about the Complainant.

July 5, 2018 E-Mail

Later, in July 2018, the Complainant e-mailed Security Manger [redacted], and VP [redacted] informing them of three upcoming Government customer site visits. The Complainant stated that the visits were extremely important, made some recommendations to prepare for the visits, and asked the group if they wanted him to take the lead on the visits because it was his understanding that there were some confidence issues with him. VP [redacted] forwarded the Complainant's e-mail to VP [redacted] and Security Director [redacted] informing them that he assumed the Complainant had taken issue with VP [redacted]'s previous feedback on an annual security self-assessment. VP [redacted] wrote that he "got the feeling that [his] inputs were very much unappreciated," and he thought the Complainant's statement was a systemic issue of an "us against them" mentality.

The Complainant told us that the lack of confidence was because the Complainant sent a data spill report to a Government customer and recommended that STR upgrade a system to a higher classification to prevent another data spill because the incident had happened previously. He told us that [redacted] yelled at him because [redacted] did not like the recommendation and pointed out that the Complainant spelled the Government program security officer's name incorrectly.

Nonetheless, the Complainant managed the site visit and received a satisfactory rating from the Government customer.

December 16, 2018 and March 4, 2019 E-Mails

VP [redacted] expressed frustration in December 2018 and March 2019 with the Complainant's numerous mistakes filling out DoD Contract Security Classification Specification forms (DD Form 254). The Complainant admitted that he made numerous mistakes because the Personnel Security group was understaffed, and he was so overwhelmed with work that he was working 50 to 60 hours per week, including weekends. He said he sent forms like the DD Form 254 up the chain, hoping someone would tell him what was wrong on the form. [redacted] told us that one of the reasons the previous security officer left STR was because the Security team was "getting crushed with work." [redacted] told us that at one point the Complainant came to him and said he was "so swamped" with SAP programs he did not have time for SCI programs. [redacted] said that he took the Complainant off the SCI programs and assigned them to himself.

September 10, 2020 E-Mail

Finally, in September 2020, VP [redacted] advised Deputy VP [redacted] that Security Director [redacted] told him the Complainant was upset and unprofessional in a meeting when the topic of office relocation was raised. [redacted] informed [redacted] in the e-mail that [redacted] and Security Manager [redacted] should have approached the security officers before the meeting to get their "buy-in" about the office seating since it was a sensitive subject.

Evidence Counter to STR's Stated Reasons for Discharge

STR provided no documentation to show that it counseled the Complainant or took steps to improve any performance issues before discharging him. [redacted] and [redacted] both explained to us that STR had an issue with its performance management process, and they acknowledged that STR failed on its documentation of performance issues at that time but has since implemented new processes.

[redacted], told us that the Complainant was very upset and continued for 5 to 10 minutes, arguing that he had not been counseled on any performance-related issues and seeking further clarification. [redacted] said that Deputy VP [redacted] gave the Complainant no real answers other than, "This is what it was."

[redacted] said that at some point during the meeting, [redacted] asked Security Manager [redacted] to speak, and he made a statement to the effect that he had not been the Complainant's supervisor that long, so he did not have anything on hand that was performance-related.

STR provided the results of a program manager survey on security officers as additional evidence of the Complainant's poor performance. On October 29, 2020, at the suggestion of Deputy VP [redacted], Security Manager [redacted] sent a survey to 22 STR program managers seeking feedback on security officers' performance. The survey asked them to rank personnel in four categories from 0 to 5. Only seven program managers responded to the survey by November 24, 2020. Of the seven, only one program manager provided feedback on the Complainant. That program manager rated the Complainant a 3 in "Impact," a 2 in "Craftsmanship," a 3 in "Teamwork," and a 2 in "Communication." [redacted] forwarded the results to VP [redacted] who replied that it was not a lot of data but that it did reveal Security Officer [redacted] and the Complainant were at the bottom.

Timing and documentary evidence indicate the survey was an attempt to gather derogatory performance data on the Complainant and Security Officer [redacted] after STR made the decision to discharge them. VP [redacted] told us that the decision to discharge the Complainant was made in late October 2020 and referred us to the e-mails STR provided. The e-mails indicate that VP [redacted] was gathering derogatory information as of October 23, 2020. Security Manager [redacted] sent the survey out on October 29, 2020, and did not receive the Complainant's only survey rating until November 2, 2020. STR did not receive [redacted]'s ratings until November 7 and 10, 2020. [redacted] called DCSA ISR [redacted] on November 4, 2020, and told him that STR was discharging the Complainant and [redacted]

Documentary evidence also indicates that VP [redacted] told DCSA ISR [redacted] that the Government was behind the discharge of the Complainant and Security Officer [redacted] On November 4, 2020, [redacted] called [redacted] and told him that STR was discharging the Complainant and [redacted] because the two customers they were supporting were not happy with their performance. STR did not present any documentary evidence or testimony to support that Government customers in 2020 had performance issues with the Complainant or [redacted]. We spoke with two DARPA program security officers who worked with the Complainant and [redacted] [redacted] and [redacted]. Neither had requested the removal of any STR personnel or expressed performance concerns. Both [redacted] and [redacted] have been DARPA program security officers since [redacted] and both were familiar with the Complainant's work at STR.

In addition, the Complainant's 2018 (January 2017 to December 2017) and 2019 (January 2018 to December 2018) annual performance reviews did not include numerical values but were positive overall. The Complainant's 2020 (January 2019 to December 2019) review did include numerical values and STR rated the Complainant 4.5 out of 5. STR gave employees quarterly bonuses based on performance, and the Complainant received a bonus for each quarter.

Four days after it discharged the Complainant and Security Officer [redacted] STR was still gathering evidence to support their discharges. Security Manager [redacted] e-mailed Deputy VP [redacted], VP [redacted] and Security Director [redacted] on November 20, 2020, with the subject line, "Feedback on [redacted] and [the Complainant]," stating, "I am a little worried, as their last manager at STR, can they file a suit/complaint against me?" [redacted] replied to all the following day stating that he was having trouble finding a "smoking gun where we said directly 'you're a horrible [Security officer]' because that has not been the culture here."

Finally, on November 24, 2020, 8 days after STR discharged the Complainant and Security Officer [redacted] Security Manager [redacted] sent a summary of the security officer survey results to VP [redacted] Security Director [redacted] and Deputy VP [redacted] Mr. McCarthy noted the seven responses were a small amount of data and asked [redacted] if they should push for more input or if it was sufficient. [redacted] replied, "I would not push harder to get more data at this point." [redacted] told us that the Complainant's single peer rating was a factor in his discharge; however, the timing and documentary evidence indicate that [redacted] made the decision to discharge the Complainant in late October 2020 before he received the survey response.

Motive to Retaliate

Evidence for motive generally exists when protected disclosures allege wrongdoing that, if proven, would adversely affect the subject. This could be true in this case, since the Complainant's protected disclosures resulted in a DCSA investigation, exposed STR's potential violations of classified security regulations to the Government customer, tarnished its reputation, and could have cost STR its multi-million-dollar DoD contracts.

Based on the testimonial and documentary evidence, we found that STR exhibited hostility toward the Complainant because of his protected disclosures.

Security Director [redacted]'s Behavior

Security Officer [redacted] submitted a complaint to STR HR on September 11, 2020, and the Complainant submitted his complaint to HR on September 13, 2020. [redacted]'s complaint focused on STR's security culture and Security Director [redacted]'s leadership style, including his direction to delay reporting the DARPA account-sharing incident to the Government. He also alleged that [redacted] demeaned employees, cursed at [redacted] in front of others, and created an environment in which members of the Security and Classified IT group

were afraid to raise concerns for fear of retaliation. The Complainant's complaint focused on [redacted]'s behavior as well; however, he also alleged that [redacted] participated in security incidents and violations that involved falsifying a report to DARPA and not properly cleaning up a data spill.

VP [redacted] and Deputy VP [redacted] conducted an investigation into the allegations made in both complaints. Their September 17, 2020 investigative report states in part that:

> [redacted] flashes signs of anger at times, exhibits vindictive behavior, holds grudges, disparages people, reprimands people in group settings, uses inappropriate language in the workplace, and doesn't empower his team to lead effectively.

The investigative report recommended that Security Director [redacted] stay in his position and that STR hire an executive coach to work with him. The report also stated, "The risk with this approach is that some of the [security officers] could leave STR."

DCSA Inquiry

The DCSA administers the National Industrial Security Program on behalf of the DoD. The DCSA opened an administrative inquiry into STR and Security Director [redacted] on August 26, 2020, based on the allegations from the Complainant's August 21, 2020 DoD Hotline complaint that was referred to the DCSA. DCSA ISR [redacted] began interviewing STR [redacted] as part of the inquiry on September 28, 2020. Two days later, CEO [redacted] sent an e-mail to the STR Board of Directors titled, "Whistleblower report to DCSA," notifying them of the DCSA inquiry and identifying the same issues that the Complainant reported in his September 13, 2020 complaint to HR.

The fact that CEO [redacted] reported Security Officer [redacted]'s and the Complainant's complaints to the Board of Directors, and STR knew the Complainant's complaint included the specific security violations that were the focus of the DCSA investigation, implies knowledge or belief that the Complainant was the source of the DCSA investigation. Before the DCSA completed its investigation or provided its results, VP [redacted] informed the DCSA on November 4, 2020, that it was discharging the Complainant and Security Officer [redacted] If the DCSA found that STR committed security violations, it could jeopardize STR's ability to work with classified information, which could damage STR's business.

Disparate Treatment of the Complainant

STR provided us a list of 12 other employees it discharged from November 2018 through November 2020. STR stated that nine of those discharges were related to unsatisfactory performance, two involved misconduct, and one employee abandoned the job.

Regarding the three security officers involved in making complaints about Security Director [redacted]:

- Security Officer [redacted] submitted an internal complaint to STR HR about Security Director [redacted]'s behavior, including his direction to delay reporting the DARPA account-sharing incident, but he did not disclose security violations outside of STR, and STR did not discharge him;
- Security Officer [redacted] also made internal complaints to STR about Security Director [redacted] but he also authored the original report to STR's Government customer, DARPA, disclosing security violations and STR's failure to report to DARPA within established timelines; and
- the Complainant disclosed security violations internally to STR, as well as to the DoD Hotline, resulting in a DCSA investigation. STR saw the Complainant as a "whistleblower" who disclosed security violations to the DCSA, triggering the investigation.

STR discharged the Complainant and Security Officer [redacted] on the same day. Both discharged STR employees were responsible for external agencies investigating STR's security practices.

The Totality of the Evidence

Weighed together, the evidence does not clearly and convincingly establish that STR would have taken the same actions absent the protected disclosures. The Complainant's disclosures to company officials resulted in internal investigations, and his disclosure to the DoD Hotline resulted in a DCSA investigation of STR's security practices. STR saw the Complainant as a whistleblower who made disclosures that resulted in the DCSA investigation.

The DCSA investigation had the potential to damage STR's reputation, hinder its ability to win future contracts, and possibly affect the security clearances of Security Director [redacted] and others. STR engaged in disparate treatment by discharging the employees who made protected disclosures outside the company but not discharging the employee who disclosed similar concerns internally.

Shortly after learning of the DCSA investigation, STR began trying to gather derogatory information to support discharging the Complainant, including initiating a survey to program managers to gather feedback on the Complainant and an October 23, 2020 e-mail in which VP [redacted] asked Security Manager [redacted] to send him any derogatory documentation he had on the Complainant.

In addition, STR's stated reasons for discharging the Complainant for poor performance were not supported by clear and convincing evidence. In fact, 4 days after STR discharged the Complainant, STR was still trying to produce documentation to support poor performance

until Deputy VP [redacted] advised that STR should not push harder to find more data. STR produced some e-mails for us, dating from 2017 through 2019, and only one from 2020, to show us the Complainant's discharge was performance-based. However, the e-mails involved minor issues that did not rise to a level for STR to formally document performance concerns or discharge him at those times. Even if the 2017 through 2019 concerns were deemed to be significant, they were too far removed to prompt the Complainant's discharge in November 2020.

VP [redacted] told the DCSA that Government customers were unhappy with the Complainant's performance. However, the only evidence STR provided to support that assertion was a 2017 e-mail indicating a customer was frustrated with STR's transition to a new security officer (the Complainant) who required training. STR initially discussed the idea of relocating security officers on September 10, 2020, 18 days before STR learned of the DCSA investigation, but STR received pushback on the idea from its security officers. It was not until STR learned of the DCSA investigation, and perceived the Complainant as the source, that it made the decision to actually move the Complainant out of his office on October 23, 2020—the same date VP [redacted] asked for derogatory documentation to support discharging the Complainant.

The office relocation hindered the Complainant from performing aspects of his duties and did not support STR's intent that alternate security officers collaborate with the security officers. The evidence further demonstrated that STR did not move the Complainant to an isolated office to minimize his risk of COVID-19 exposure. Rather, the evidence supported that STR removed the Complainant from the Area 1 Security office to an isolated office because STR considered him a problem and knew that it would be discharging him. Although STR discussed the office relocations before the Complainant made several disclosures, including the one that resulted in the DCSA investigation, that decision stalled. It was not until STR made the decision to discharge the Complainant that it made the final decision to actually move him.

Finally, the Complainant's 2020 annual review rating was 4.5 out of 5, and he received all of his performance-based quarterly bonuses throughout his tenure at STR. These facts contradict STR's stated reasons for its decision to discharge him for poor performance.

Conclusion

In the absence of clear and convincing evidence to the contrary, the evidence establishes that STR relocated the Complainant's office and discharged him in reprisal for his protected disclosures.

Recommendations

We recommend that the Secretary of the Navy direct Navy officials to:

- consider appropriate action against STR for reprising against the Complainant; and
- order STR to award the Complainant compensatory damages (including back pay), employment benefits, and other terms and conditions of employment that the Complainant would have received had he not been reprised against.

Acronyms and Abbreviations

CEO	Chief Executive Officer
COVID-19	Coronavirus Disease–2019
CSA	Cognizant Security Agency
DARPA	Defense Advanced Research Project Agency
DCSA	Defense Counterintelligence and Security Agency
FBI	Federal Bureau of Investigation
FDA EUA	Federal Drug Administration Emergency Use Authorization
FSO	Facilities Security Officer
HR	Human Resources
IT	Information Technology
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program: Operating Manual
PCR	FDA EUA-approved molecular COVID-19 test
SAP	Special Access Programs
SCI	Sensitive Compartmented Information
STR	Systems & Technology Research, LLC
U.S.C.	United States Code
VP	Vice President


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

~~CUI~~

Whistleblower Reprisal Investigation
D-CATSe 20201124-068294-CASE-01

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

~~CUI~~