~~Sensitive Material~~

The Inspector General of the Department of the Air Force

Report of Investigation (S9691)

Unauthorized Disclosure of National Security Information

August 2023

~~DO NOT OPEN COVER WITHOUT A NEED TO KNOW-- PROTECTED COMMUNICATION TO IG~~

EXECUTIVE SUMMARY

SecAF directed this investigation in response to the unauthorized disclosure of classified information from the 102d Intelligence Wing (102 IW), Otis Air National Guard Base (ANGB), Massachusetts. SecAF directed The Inspector General of the Department of the Air Force (SAF/IG) to "investigate compliance with policy, procedures, and standards and the unit environment at the 102 IW related to the unauthorized disclosure of classified national security information." While the precipitating event was centered on the 102 IW, the investigation included organizations and areas outside the 102 IW regarding security-related policies and procedures. Although related, this administrative investigation is separate from the criminal investigation currently being led by the Department of Justice (DOJ).

On 13 Apr 23, Federal Bureau of Investigation (FBI) agents from the Boston Field Office arrested A1C Jack D. Teixeira, a Cyber Transport Systems Apprentice in the Massachusetts ANG (MAANG), on suspicion of willfully retaining and transmitting classified national defense information to a person not entitled to receive it via Discord, a social media platform. A1C Teixeira enlisted in the USAF on 26 Sep 19, and his Top Secret-Sensitive Compartmented Information (TS-SCI) background check was adjudicated on 29 Jun 21. On 1 Oct 21, he began the first of two consecutive in-place Title 10 (T10) tours. As a computer/IT specialist in the 102d Intelligence Support Squadron (102 ISS), A1C Teixeira had access to numerous classified systems, including the Joint Worldwide Intelligence Communication System (JWICS), a TS-SCI platform, to perform system maintenance. His access to JWICS enabled him to view intelligence content and analysis that reside on those systems.

A1C Teixeira was reportedly involved in an online chat group on Discord discussing geopolitical affairs and current and historical wars. FBI currently assesses A1C Teixeira started to post classified information as early as Feb 22. Initially, A1C Teixeira was allegedly posting rewritten "paragraphs of text." Then, around Jan 23, he allegedly started posting photographs of documents that contained Top Secret classification markings and described the status of a current military conflict, including troop locations. A1C Teixeira reportedly stated he was concerned he would be discovered making the transcriptions in the secure work center on Otis ANGB, so he began taking the documents home to photograph and post online.

Evidence indicates the primary cause of the unauthorized disclosure is the alleged actions of one individual, A1C Teixeira, who is suspected to have violated trust and security protocols to unlawfully disclose national security information. Determining A1C Teixeira's motives and actions remain the focus of the DOJ and FBI efforts. However, there are also a number of factors, both direct and indirect, that contributed to the unauthorized disclosures.

Direct Contributing Factors

Evidence indicates some members in A1C Teixeira's unit, reporting chain, and leadership had information about as many as four separate instances of his questionable activity. A smaller number of unit members had a more complete picture of A1C Teixeira's intelligence-seeking behaviors and intentionally failed to report the full details of these security concerns/incidents as outlined in DoD security policies, fearing security officials might "overreact." Had any of these members come forward, security officials would likely have facilitated restricting systems/facility access and alerted the appropriate authorities, reducing the length and depth of the unauthorized and unlawful disclosures by several months.

IT specialists in the 102 ISS, including A1C Teixeira, were encouraged to receive weekly intelligence briefings to better understand the mission and the importance of keeping the classified networks operating. This "know your why" effort was improper in that it provided higher level classified information than was necessary to understand the unit's mission and created ambiguity with respect to questioning an individual's need to know. Around July or August of 2022, A1C Teixeira was observed viewing intelligence content on TS-SCI websites. His supervisor was informed, but the incident was not documented in writing. Then, on 15 Sep 22, a unit member noticed A1C Teixeira again viewing intelligence products and saw him writing information on a post-it note. A1C Teixeira was confronted about the note and directed to shred it. However, it was never verified what was written on the note or whether it was shredded. His supervisor and another unit member documented the event via Memorandum for Record (MFR), and A1C Teixeira was directed to stop taking notes on classified information and "to cease all research where he did not have a need to know." These incidents were not reported to the proper security official.

One month later, on 25 Oct 22 during an intelligence briefing, A1C Teixeira asked very detailed questions and even attempted to answer questions using suspected TS-SCI information he did not have a need to know. Leadership who was present questioned the classification level of the information he was citing, and A1C Teixeira stated the information was classified but added it was also available via "open sources." Contrary to his assertion, the information was not believed to be publicly available and A1C Teixeira's supervisor was again advised of his suspected intelligence-seeking behavior. A1C Teixeira was again ordered to "cease and desist" intelligence "deep dives." This third incident was documented with another MFR, but not reported to the proper security official.

On 30 Jan 23, a unit member observed A1C Teixeira viewing intelligence content again after being previously ordered to cease and desist. The supervisor was informed, an MFR was written, and more senior members of the squadron's leadership were made aware of three of the four preceding incidents. After some internal discussion, a substantially minimized version of the concerns was provided to security officials. The security officials were not provided copies of the MFRs or an accurate description of the security concerns. As a result, additional available

security actions were not taken and no further inquiry or investigation occurred. After interviewing higher levels of the supervisory chain, it appears knowledge of these security incidents was not fully disclosed above the squadron level. Based on the preponderance of the evidence gathered during the investigation, three individuals in the unit who understood their duty to report specific information regarding A1C Teixeira's intelligence-seeking and insider threat indicators to security officials, intentionally failed to do so.

Indirect Contributing Factors

A number of indirect contributing factors enabled the occurrence and duration of the improper collection and unauthorized release. A brief summary of each of those factors is provided below.

Inconsistent Reporting Guidance. DoD and AF guidance clearly states actual and potential compromises involving SCI must be reported to the proper security official. However, guidance on reporting security incidents, in general, is inconsistent across DoD and AF Instructions/Manuals, allowing for reporting to the supervisory chain and/or security personnel depending on the level of classified information. This inconsistency, coupled with the total number of governing regulations regarding security, created misconceptions and misunderstanding in the 102 IW on reporting suspicious behavior and security infractions. Some members mistakenly believed they could report violations to their supervisors (chain of command) and/or other officials, instead of the proper security official, as required in this case.

Conflation of Classified System Access with "Need to Know" Principle. Evidence indicates some personnel, when faced with how to enforce need to know, believed having a TS-SCI clearance and access to classified systems meant users had approval to examine any information they could find on JWICS. Mistakenly, many personnel disregarded the requirement to have a valid need to know and did not ensure the information was properly determined to be essential to effectively carry out their official duties and assignments. As a result, there was a lack of robust validation regarding the need to know. Computer/IT specialists require system access to perform system maintenance, but do not require access to intelligence content or products to maintain the system.

Inconsistent Need to Know Guidance. Evidence indicates a lack of understanding of the need to know concept due to inconsistent guidance on the topic. In most cases, the concept of need to know is presented as a responsibility of the individual granting access to classified information. For example, Executive Order 12968, 2 Aug 95, defines need to know as a determination made *by an authorized holder of classified information* that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. This approach has become insufficient with the growing abundance and access to digitally-based classified information. The need to know principle has appropriately expanded, but only in a limited number of security standards. Specifically, with

respect to TS-SCI, need to know includes the principle that individuals may only acquire information essential to effectively carry out their assigned duties.

Differences in Disciplinary Action Between Title 32 (State) and Title 10 (Federal) Members. To support its federal mission, numerous 102 IW members are placed in Title 10 (T10) status and are assigned to the 201st Mission Support Squadron (201 MSS) at Joint Base Andrews, MD, for administrative control, including disciplinary actions. Title 32 (T32) commanders can complete disciplinary actions on T32 Airmen locally using the Massachusetts Code of Military Justice (MCMJ). However, by Air Force Instructions and 201 MSS policy, disciplinary actions for T10 personnel had to be coordinated with the 201 MSS prior to taking action. According to some witnesses, this coordination process took additional time to accomplish disciplinary actions and it was believed this affected good order and discipline. As a result, frontline supervisors might seek to avoid coordinating with the 201 MSS entirely by simply opting to give verbal counselings or writing informal MFRs instead of more appropriate forms of documented disciplinary action. The use of other forms of documentation, such as the MFR, effectively bypassed existing standards for progressive discipline, leaving a number of Airmen collecting MFRs and not receiving appropriate command and security oversight.

Lack of Supervision/Oversight of Night Shift Operations. Evidence indicated a lack of supervision during night shifts. When there were no intelligence missions at night, members of a three-person crew, like the one A1C Teixeira was on, were the only personnel in the open-storage TS-SCI facility. Their primary role was to ensure the Heating, Ventilation, and Air Conditioning (HVAC) system was operating properly and answer the phones. At times, members were required to perform preventive maintenance inspections and other tasks, which required individuals to be on their own for hours, unsupervised in other parts of the facility. Further, no permission controls were in place to monitor print jobs, and there were no business rules for print products. Any night shift member had ample opportunity to access JWICS sites and print a high volume of products without supervision or detection.

Results of Defense Counterintelligence and Security Agency (DCSA) Field Investigations for Security Clearances Not Provided to Units. All members with a security clearance require a background check. However, the details learned in background checks are not routinely shared with a member's unit. During A1C Teixeira's background check, some negative information was discovered. The adjudication service, utilizing the "whole person" concept and federal guidelines, granted him a favorable determination for a TS-SCI clearance and notified the 102 IW. While information in A1C Teixeira's background check did not ultimately preclude him from receiving his clearance, there were indications that A1C Teixeira could have been subject to enhanced monitoring. In addition, had the unit been made aware of potential security concerns identified during the clearance adjudication process, they may have acted more quickly after identifying additional insider threat indicators.

Compliance/Self Inspection

The Air Force Inspection Agency (AFIA) conducted an independent inspection through a review of data provided by the 102 IW, an on-site evaluation of specific programs, functional and leadership interviews, and Group Airmen-to-IG Sessions (ATIS-G) of unit members to assess the 102 IW culture regarding security and protection of classified information. Based upon these reviews, the preponderance of the evidence shows that 102 IW and 102 ISRG commanders were not vigilant in inspecting the conduct of all persons who were placed under their command.

Protection of SCI Material and Information Security (INFOSEC) Programs. The 102 IW INFOSEC program was not effective and lacked meaningful activity prior to 2023. Wing and group leadership prioritized immediate mission requirements, such as processing personnel clearances and granting access, but did not provide necessary support or resources to accomplish program responsibilities fully and effectively. There was a lack of INFOSEC inspection emphasis by 102 IW leadership.

Intelligence Oversight (IO) Program Found Compliant but Lacking. Although AFIA found the IO program "in compliance," there were notable non-compliant exceptions. In particular, many 102d Intelligence, Surveillance, and Reconnaissance Group (102 ISRG) members had not completed IO training. Supervisors did not facilitate the reporting of known and possible IO-associated violations or irregularities. Finally, the unit's inconsistent enforcement of compliance with IO was concerning.

Unit Self-Assessment Program (USAP). The 102 IW did not have a well-communicated, actioned, or enforced USAP. Inspection data since 2020 showed known concerns and insufficient program improvement from wing, group, and squadron levels that should have been apparent to wing leadership. Although business rules state the relative importance of self-inspection, actions show leadership did not apply or enforce wing or group level direction. Interviews with personnel indicated a lack of awareness and understanding of the program at all levels. A more rigorous self-assessment program may have identified the INFOSEC and IO issues that contributed to this unauthorized disclosure.

Unit Security Climate. AFIA completed ATIS-G sessions to collect feedback from 199 personnel, including both full- and part-time military members, to assess the security climate across the 102 IW. Of those, 80% felt that security-related training was ineffective, needed to be removed from the wing's annual training day, where numerous mandatory training items are completed, and should shift to group discussions to give this critical topic greater emphasis. Many members highlighted the need for more practical application of security training, including internal exercises. Additionally, there appeared to be a culture of complacency within these units. For example, members described trusting their coworkers without verifying access or need to know and inconsistently practicing certain disciplines like locking classified computer

terminals when leaving their desks. Members further described this culture by emphasizing the frequency of entry "tailgating" and unenforced badge wear while on the ops floor. Finally, feedback indicated leaders' focus on completing tasks not directly mission-related, with minimal resources, created a critically permissive culture that reinforced risk-accepting behaviors at inappropriate levels.

Additional Considerations

The role the DAF Counter-Insider Threat Hub (DAF C-InT Hub) played, or should have played, in this event was also analyzed. The DAF C-InT Hub is tasked to collect, integrate, and analyze indicators of potential insider threats from multiple sources, to include monitoring, audit management, cybersecurity, law enforcement, counterintelligence, personnel security, human resources, command reporting, and the medical and legal communities. When properly executed, an Airman reports an insider threat concern to the wing Information Protection Office (IPO), who forwards it to the MAJCOM IPO/Insider Threat Liaison, who then files a report with the DAF C-InT Hub. Proper, early notifications to security officials in this case and the ability to proactively identify anomalous behavior would have leveraged the full capabilities of the DAF C-InT Hub.

Summary

The primary cause of the unauthorized disclosure is the alleged deliberate actions of one individual, A1C Teixeira. However, there were also a number of contributing factors, both direct and indirect, that enabled the unauthorized disclosures to occur and continue over an extended period of time.

The preponderance of the evidence shows three individuals in A1C Teixeira's supervisory chain had information about as many as four separate instances of security incidents and potential insider threat indicators they were required to report. Had any of these three members come forward and properly disclosed the information they held at the time of the incidents, the length and depth of the unauthorized disclosures may have been reduced by several months.

The preponderance of the evidence also shows that 102 IW and 102 ISRG commanders were not vigilant in inspecting the conduct of all persons who were placed under their command. Specifically, an inspection of areas related to security and protection of classified information through on-site evaluation of specific programs and interviews of unit members, revealed that wing and group leadership prioritized immediate mission security requirements, but did not take required actions to accomplish security program responsibilities fully and effectively.

Additionally, information technology specialists, including A1C Teixeira, were encouraged to receive weekly intelligence briefings to better understand the mission and the importance of keeping the classified network operating. This "know your why" effort was

improper in that it provided higher level classified information than was necessary to understand the unit's mission and created ambiguity with respect to questioning an individual's need to know.

Finally, indirect factors including inconsistent security reporting guidance, conflation of classified system access and the "Need to Know" principle, inconsistent guidance on the "Need to Know" concept, deficiencies in the T10 disciplinary process, lack of adequate supervision and oversight of night shift operations, and lack of visibility into the negative factors discovered during the initial Defense Counterintelligence and Security Agency (DCSA) field investigation also contributed to this unauthorized disclosure.