~~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.

TABLE OF CONTENTS

REPORT OF INVESTIGATION (Case S9691)

CONCERNING

UNAUTHORIZED DISCLOSURE OF NATIONAL SECURITY INFORMATION

PREPARED BY
SAF/IGS
August 2023

I. INTRODUCTION

The Secretary of the Air Force (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), MA. (Ex 1) 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 102d Intelligence Wing related to the unauthorized disclosure of classified national security information." (Ex 1) While the precipitating event was centered on the 102 IW, the investigation included organizations and matters 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).

The investigating team prepared an Investigation Plan (IP) and presented the IP to The Inspector General on 24 Apr 23. During this investigation, the following individuals provided sworn testimony regarding the allegations covered in this report:

- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)

- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)

The following individuals also provided sworn statements and/or provided information regarding the allegations and issues covered in this report:

- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)

- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C)

II. BACKGROUND

On 13 Apr 23, Federal Bureau of Investigation (FBI) agents from the Boston Field Office arrested Massachusetts Air National Guard (MAANG) member A1C Jack Douglas Teixeira, a Cyber Transport Systems Apprentice,[1] at his residence in North Dighton, MA, 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. (Ex 81:5; Fig 1)

A1C Teixeira enlisted in the United States Air Force (USAF) on 26 Sep 19, and his Top Secret-Sensitive Compartmented Information (TS-SCI) eligibility was adjudicated on 29 Jun 21. (Ex 82:2; Ex 84) As a computer/Information Technology (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. (Ex 81:6) On 1 Oct 21, he began the first of two consecutive in-place Title 10 (T10) tours at Otis ANGB. (Ex 85) In a T10 status, A1C Teixeira's administrative chain of command for disciplinary actions was the 201st Mission Support Squadron (201 MSS), Joint Base (JB) Andrews, MD, and not the 102 IW. (Ex 114)

A1C Teixeira was reportedly involved in an online chat group, on the social media platform Discord, discussing geopolitical affairs and current and historical wars. On 10 Apr 23, the FBI interviewed users of the social media platform, and currently assesses A1C Teixeira started posting classified information as early as Feb 22. (Ex 127) Initially, A1C Teixeira was allegedly posting rewritten paragraphs of text. Then, around Jan 23, he allegedly started posting photographs of documents which contained Top Secret classification markings. According to an FBI witness, documents posted described the status of a current military conflict, including troop movements. 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 them online. (Ex 81:4-5; Ex 126; Ex 127)

On 25 Apr 23, The Inspector General of the Department of the Air Force (SAF/IG) and a team of experts from the Senior Official Inquiries Directorate (SAF/IGS), Air Force Inspection Agency (AFIA), The Office of the Judge Advocate General (AF/JA), and Air Force ISR and Cyber Effects Operations (AF/A2/6) traveled to Otis ANGB to inspect and investigate the 102 IW's compliance with security procedures and standards and assess the environment in which A1C Teixeira was able to routinely access and release national security information over an extended period of time, undetected. It is important to note, A1C Teixeira is a computer/IT specialist assigned to the 102 ISS, and not an intelligence analyst. He required access to classified systems to perform system maintenance, but that access also enabled him to view intelligence content and analysis that reside on those systems, which he did not need to know.

[1] The Air Force Specialty Code (AFSC) for a Cyber Transport Systems Apprentice is 1D751A

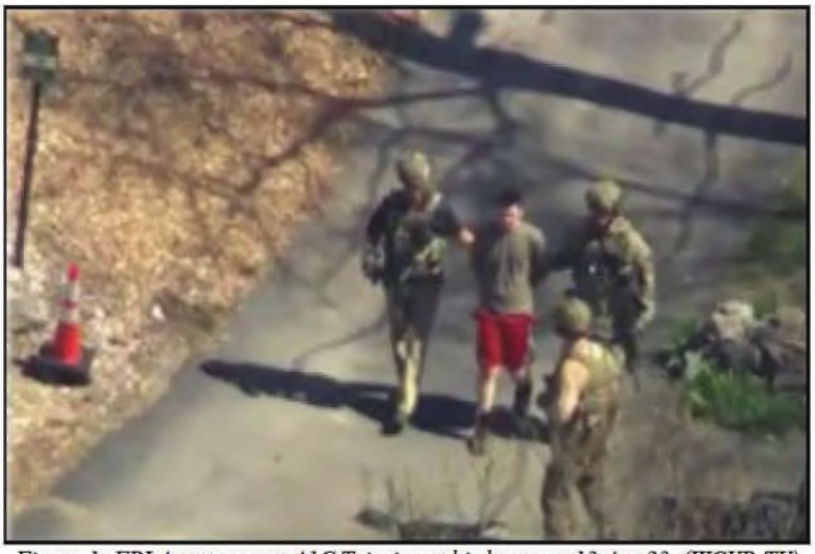

Figure 1: FBI Agents arrest A1C Teixeira at his home on 13 Apr 23. (WCVB-TV)

National Guard

The National Guard has a unique dual mission, with both federal (Title 10 U.S.C.) and state (Title 32 U.S.C.) responsibilities.[2] There are Army National Guard and Air National Guard units and personnel in each of the 50 States, the territories of Puerto Rico, the Virgin Islands, and Guam, and the District of Columbia. Under Title 32, when authorized or directed by the President, the governor can call the National Guard into action during local or state-wide emergencies, such as storms, droughts, and civil disturbances. In addition, the President can activate the National Guard to participate in federal missions, both domestically and overseas. When federalized under Title 10 authority, Guard units fall under the same military chain of command as active duty and reserve personnel. When not called for federal active service, the governors serve as the Commanders-in-Chief for the National Guard in their respective states and territories (with the exception of the DC National Guard). (Ex 131) The Adjutant General (TAG) for each state and territory, in most cases, reports directly to their Governors, and under state authorities may be designated as a commander for their respective state. (Ex 131)

The National Guard Bureau (NGB) is a joint activity of the Department of Defense and is led by the Chief, National Guard Bureau (CNGB). NGB is not a command; as such, it has no command authority over the National Guard in the several states. DODD 5105.77 says, "The NGB is the focal point at the strategic level for non-federalized National Guard matters that are not the responsibility of the Secretary of the Army, the Secretary of the Air Force, or the CJCS, in law or DoD policy." (Ex 132:2)

[2] Title 32 is full-time National Guard duty while Title 10 is full-time Active duty. Title 10 positions are generally federal level jobs, while Title 32 jobs are at the state level.

102d Intelligence Wing and Subordinate Units

102d Intelligence Wing (102 IW)

The 102 IW, Otis ANGB, MA, is responsible for the activities of 1,260 military and civilian personnel prepared to respond to domestic emergencies in the Commonwealth of Massachusetts, while training and maintaining readiness to accomplish wartime missions of intelligence, surveillance, and reconnaissance operations, cryptologic intelligence, cyber engineering and installation support, medical, and expeditionary combat support. (Ex 8:1)

The mission of the 102 IW is "to organize, administer, recruit, instruct & train ready personnel/equipment to meet federal or domestic tasking requirements, for employed-in-place missions, expeditionary combat support or in resource to state requests for forces." (Ex 106:1) There are five subordinate groups under the 102 IW, including the 102d Intelligence, Surveillance and Reconnaissance Group (ISRG), as depicted here:

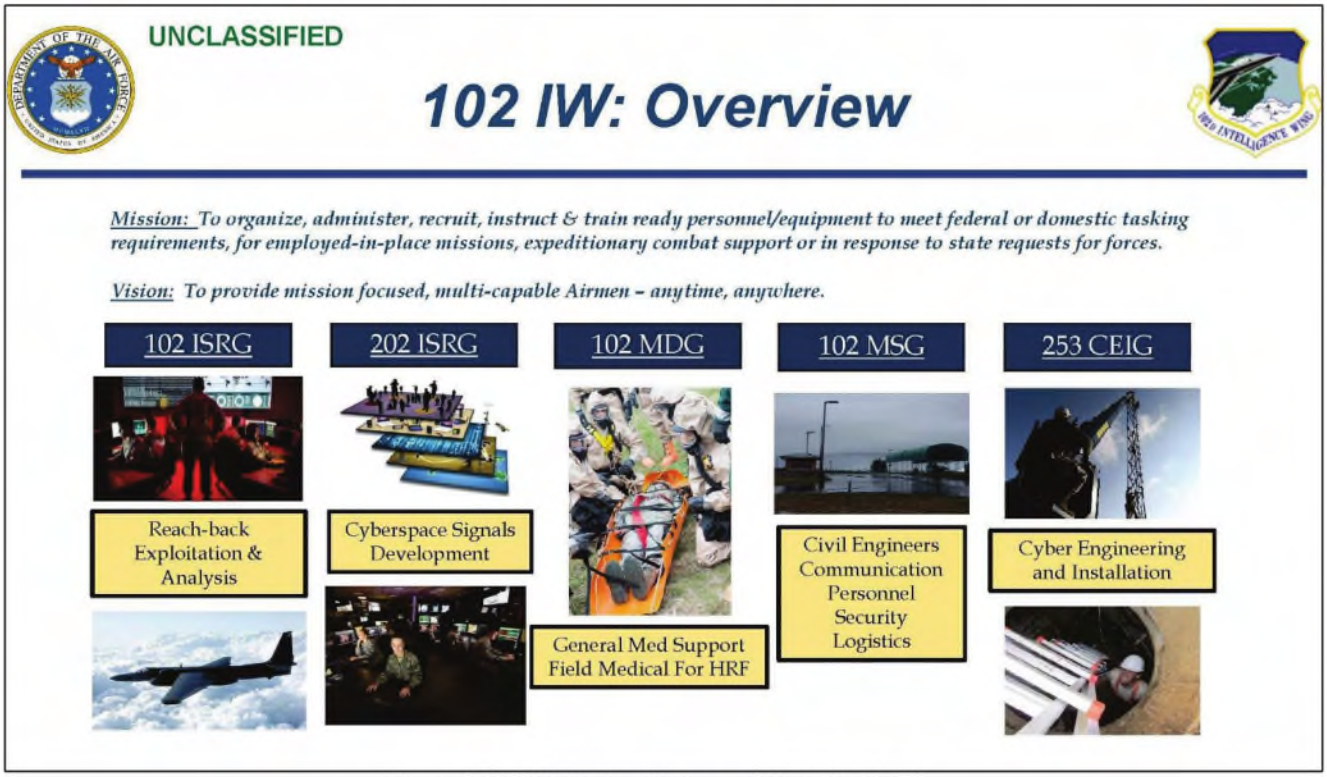

Figure 2: 102 IW Mission, Vision, and Units (Ex 106:1)

102d Intelligence, Surveillance and Reconnaissance Group (102 ISRG)

The 102 ISRG is a subordinate unit of the 102 IW and is the parent organization for the 101st Intelligence Squadron (IS), 102d Intelligence Support Squadron (ISS), and the 102d Operations Support Squadron (OSS). (Ex 4)

Air Force Distributed Common Ground System (AF DCGS)

AF DCGS, also referred to as the AN/GSQ-272 SENTINEL weapon system, is the Air Force's primary ISR planning and direction, collection, processing and exploitation, analysis, and dissemination (PCPAD) weapon system. The weapon system employs a global communications architecture that connects multiple intelligence platforms and sensors. Airmen assigned to AF DCGS produce actionable intelligence from data collected by a variety of sensors on the U-2, RQ-4 Global Hawk, MQ-1 Predator, MQ-9 Reaper, and other ISR platforms. (Ex 13)

Distributed Ground System-Massachusetts (DGS-MA)

The 102 ISRG, DGS-MA, is one of 27 regionally aligned, globally networked sites, 11 of which are assigned to the ANG. (Ex 13; Ex 126) The sites have varying levels of capability and capacity to support the intelligence needs of the warfighter. A DGS is capable of robust, multi-intelligence processing, exploitation, and dissemination (PED) activities to include sensor tasking and control. It can support multiple ISR platforms in multiple theaters of operation simultaneously. (Ex 126) Operationally, DGS-MA falls under the 480th Intelligence, Surveillance and Reconnaissance Wing (480 ISRW) located at Langley AFB, Virginia, and is comprised of more than 370 assigned military and civilian Airmen and contractors. (Ex 4)

101st Intelligence Squadron (101 IS)

The 101 IS conducts real-time tactical and national intelligence collection, exploitation, analysis, and reporting operations. The squadron partners with and directs U-2 Dragon Lady, MQ-9 Reaper, and RQ-4 Global Hawk aircraft in order to develop intelligence products from the data collected and produce cryptologic and imagery products for war fighters and decision makers operating in, or concerned with, the U.S. Central Command (CENTCOM), U.S. European Command (EUCOM), U.S. Africa Command (AFRICOM), and U.S. Special Operations Command (SOCOM) areas of responsibility. (Ex 130)

102d Intelligence Support Squadron (102 ISS)

The 102 ISS is one of three units that make up the 102 ISRG and DGS-MA at Otis ANGB. The squadron is comprised of more than 100 military, civilian, and Contract Field Support Representative (CFSR) Cyberspace Support professionals.

In performing its federal mission, the 102 ISS provides intelligence systems maintenance, integration, and operations for the AN/GSQ-272 SENTINEL weapon system, as part of the AF DCGS Enterprise, enabling near real-time Collection, Processing, Exploitation, and Dissemination (CPED) of fused intelligence to warfighters, combatant commanders, and the larger intelligence community. The weapon system employs a global communications architecture that connects multiple airborne intelligence collection platforms and sensors to Imagery and Signals Intelligence Analysts at Otis ANGB and other DGS sites. The 102 ISS ensures the availability and integrity of weapon system networks, 24 hours a day, 365 days a year, through operation and maintenance of mission and ancillary networks and equipment, software installation and support, information system security, communications security, technology integration and innovation, systems architecture and configuration management, supply and logistics, and contract management and oversight. In addition, the 102 ISS provides support to the overall maintenance effort of the North American Aerospace Defense Command (NORAD) Pocket J Situational Awareness Data Link (SADL) system at Otis ANGB.

While performing its state mission, the 102 ISS maintains an Unclassified Processing, Awareness and Dissemination (UPAD) system in support of 102 IW Domestic Operations (DOMOPS) missions.

Key Duty Descriptions

Special Security Office or Officer (SSO) – manages the Sensitive Compartmented Information (SCI) security program and oversees SCI security functions for subordinate SCI Facilities (SCIF). (Ex 17:12)

Information System Security Manager (ISSM) – serves as the primary cybersecurity technical advisor and manages the cyber security program. (Ex 29:25)

Information System Security Officer (ISSO) – responsible for ensuring the appropriate operational security posture is maintained for the assigned Information Technology (IT). (Ex 26:15)

Information Protection (IP) – consists of a set of three core security disciplines (Personnel, Industrial, and Information Security) used to: 1) determine personnel's eligibility to access classified information or occupy a sensitive position; 2) ensure the protection of classified

information; and 3) protect classified information that, if subject to unauthorized disclosure, could reasonably be expected to cause damage to national security. (Ex 26:11)

Air Force Counter-Insider Threat Hub (AF C-InT Hub)

The AF C-InT Hub is the DAF's centralized risk analysis center. It is tasked to collect, integrate, and analyze indicators of potential insider threats from multiple sources, to include User Access Monitoring (UAM), enterprise audit management, cybersecurity, law enforcement, counterintelligence, personnel security, human resources, command reporting, and medical and legal communities. (Ex 27:10)

III. CHRONOLOGY

DATE	EVENT
26 Sep 19	A1C Teixeira enlisted in the MAANG for a 6-year period. (Ex 84)
29 Jun 21	A1C Teixeira's TS-SCI eligibility was adjudicated. (Ex 82:2)
o/a Summer 21	A1C Teixeira told another A1C in his squadron he was denied a Firearms ID Card (FID)[3] because of rumors in high school that he "threatened to shoot up the school," according to a witness. The comments were reported to squadron leadership during a training meeting. (Ex 67:2)
1 Oct 21	A1C Teixeira is placed on Active Duty T10 orders from 1 Oct 21 to 30 Sep 22 at Otis ANGB in support of Operation INHERENT RESOLVE (OIR). (Ex 85:1-4) While serving on T10 orders, A1C Teixeira is assigned to the 201 MSS for Administrative Control (ADCON) and is subject to the Uniform Code of Military Justice (UCMJ). (Ex 85:1)
o/a Feb 22	A1C Teixeira allegedly began posting classified information online, primarily on the social media platform Discord. (Ex 127)
o/a Mar 22	A1C Teixeira's mission crew lead expressed concerns to A1C Teixeira's supervisor about A1C Teixeira having the potential to be an active shooter based on conversations with him about machine guns, suppressors, explosives, living off the grid, etc. (Ex 68:1)
13 Jul 22	An external Blu-Ray drive (with read/write capability) used for performing system maintenance was plugged into a JWICS machine while connected to the network. Nine users were logged into the machine at the time, including A1C Teixeira. None of the users admitted to the violation. (Ex 88:1)

[3] A FID is required to purchase firearms in MA; the application process includes a background check. (Ex 120)

o/a Jul/Aug 22	The (b) (6), (b) (7)(C) witnessed A1C Teixeira viewing intelligence content on JWICS instead of focusing on his primary duties and brought these concerns to A1C Teixeira's supervisor. (Ex 38:35-36) This matter was not documented.
31 Aug 22	A1C Teixeira failed his annual Fitness Assessment. (Ex 92)
15 Sep 22	An Imagery Analyst witnessed A1C Teixeira viewing intelligence products and a map on JWICS and saw him writing down information from the map onto a post-it note. A SNCO became aware and reported the matter to A1C Teixeira's supervisor, and they both documented the incident with MFRs. (Ex 89; Ex 90) The supervisor directed A1C Teixeira "to cease all research where he did not have a need to know." (Ex 44:44; Ex 50:2)
1 Oct 22	A1C Teixeira was placed on another set of Active Duty T10 orders from 1 Oct 22 to 30 Sep 23 at Otis ANGB in support of Operation SPARTAN SHIELD. (Ex 85:5-6) To date, he remains assigned to the 201 MSS for ADCON and is still subject to the UCMJ. (Ex 114)
25 Oct 22	During an intelligence briefing, A1C Teixeira asked detailed questions and attempted to answer questions using suspected TS-SCI information for which he did not have a need to know. (Ex 91) The (b) (6), (b) (7)(C) questioned the source of the information, and A1C Teixeira explained it was both classified and publicly available ("open source"[4]). A1C Teixeira's supervisor again ordered him to "continue to cease and desist" intelligence "deep dives," and another enlisted member documented the incident with an MFR. (Ex 50:2; Ex 91) Following this incident, A1C Teixeira's supervisor asked the ISSOs if they could scan the network to "see what [A1C Teixeira] was looking at," and was told that was not a capability they have. (Ex 41:25-28)
27 Oct 22	The (b) (6), (b) (7)(C) [5] issued A1C Teixeira a Letter of Counseling (LOC) for his 31 Aug 22 Fitness Assessment failure. (Ex 92)

[4] Open-source intelligence (OSINT) is intelligence that is produced from publicly available information. Reference https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap15-subchapI-sec403-5.htm.

[5] (b) (6), (b) (7)(C) was dual hatted as the (b) (6), (b) (7)(C) members serving in T10 status. The (b) (6), (b) (7)(C) was delegated Administrative Control (ADCON) authority, which included disciplinary actions, by the (b) (6), (b) (7)(C). (Ex 37:35-36; Ex 118)

o/a Dec 22, 0600-0700	102d Security Forces Squadron (102 SFS), responded to a call at the 102 ISRG after A1C Teixeira left his unattended car running in the parking lot for a long period of time. The responding officer noticed multiple shooting targets and a large military-style backpack in the rear seat. Once A1C Teixeira arrived at the car, he said the officer could search his vehicle. The officer did not feel it was necessary to search the vehicle, so he declined, and A1C Teixeira departed the scene. A1C Teixeira's supervisor later called the responding officer to tell him that the squadron was keeping documentation on A1C Teixeira because they believed something was suspicious about his conduct. The officer told the supervisor to file a report of anything wrong or suspicious to SFS; no report was filed. (Ex 98:1-2)
1 Jan 23	A1C Teixeira failed to report to his regular shift at 0630 and did not respond to phone calls from his crew lead or his supervisor. A1C Teixeira reported to work at 0830, two hours late. The supervisor documented this incident via MFR. (Ex 94)
o/a Jan 23	A1C Teixeira's crew lead overheard a conversation between the [redacted] and A1C Teixeira's supervisor about A1C Teixeira being late again and heard them make a vague reference to A1C Teixeira accessing information without a need to know. They also discussed A1C Teixeira having the potential to be an active shooter. (Ex 68:2)
o/a Jan 23	A1C Teixeira allegedly began posting photographs of documents containing classified markings online. A1C Teixeira reportedly told a fellow Discord user 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. (Ex 81:5)
30 Jan 23	A SNCO observed A1C Teixeira viewing intelligence content on JWICS again, after being previously ordered to cease and desist. (Ex 95) [redacted] notified A1C Teixeira's supervisor and documented it with another MFR on 4 Feb 23. (Ex 95) The [redacted] and the [redacted] were made aware of three of the four preceding incidents, which were documented in MFRs. (Ex 44:26) The [redacted] informed the [redacted] that [redacted] would notify the [redacted]. (Ex 36:108) However, the [redacted] failed to adequately notify the SSO of the security concerns. (Ex 43:172)
31 Jan 23	A1C Teixeira's supervisor ordered A1C Teixeira to report to Regularly Scheduled Drill (RSD) at 0700 to receive his flu shot; A1C Teixeira failed to report as ordered. (Ex 96) The supervisor issued A1C Teixeira a Record of Individual Counseling (RIC) on 4 Feb 23 for this incident. (Ex 96)

o/a Feb/Mar 23	A1C Teixeira's supervisor called another enlisted member into the office of the (b) (6), (b) (7)(C) [redacted]. (Ex 67:3) With the (b) (6), (b) (7)(C) [redacted] present, the supervisor asked the other enlisted member, "Have you heard about this story about Teixeira, about him in high school?" (Ex 67:3) The enlisted member said [redacted] heard the story, and reminded the supervisor [redacted] told him and the squadron leadership about it back in 2021. (Ex 67:3)
2 Mar 23	A1C Teixeira missed a scheduled training event. (Ex 46:41-42) When his supervisor asked why he missed his training, A1C Teixeira provided an unprofessional and crass response. (Ex 97) His supervisor documented this incident via MFR on 3 Mar 23. (Ex 97)
13 Apr 23	FBI agents arrested A1C Teixeira at his Massachusetts home. (Ex 81:5)

IV. ANALYSIS

STANDARDS.

Executive Order 12968, *Access to Classified Information*, 7 Aug 95

Security Executive Agent Directive 3 (SEAD 3), *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*, 12 Jun 17

Security Executive Agent Directive 4 (SEAD 4), *National Security Adjudicative Guidelines*, 8 Jun 17

DoDM 5105.21V1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*, 19 Oct 12, IC 2, Eff 6 Oct 20.

DoDM 5105.21V3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities*, 19 Oct 12, IC 2, Eff 14 Sep 20

DoDM 5200.01V1_AFMAN 16-1404V1, *Information Security Program: Overview, Classification, and Declassification,* 6 Apr 22

DoDM 5200.01V3_AFMAN 16-1404V3, *Information Security Program: Protection of Classified Information,* 12 Apr 22

DoDM 5200.02_AFMAN 16-1405_AFGM2022-03, *AF Personnel Security Program,* 30 Nov 22

DoDD 5205.16, *The DoD Insider Threat Program*, 30 Sep 14, IC2, 28 Aug 17

AFI 10-701, *Operations Security,* 24 Jul 19

AFMAN 14-403, *Sensitive Compartmented Information Security and Intelligence, Surveillance and Reconnaissance Systems Cybersecurity and Governance,* 3 Sep 19

AFI 14-404, *Intelligence Oversight*, 3 Sep 19

DAFI 16-1401, *Information Protection Program,* 3 Feb 23

AFI 16-1402, *Counter-Insider Threat Program Management,* 17 Jun 20

ANGI 36-101, *Air National Guard Active Guard and Reserve (AGR) Program*, 21 Apr 22

DoD Manual 5200.01V1_DAFMAN 16-1404V1, *Information Security Program: Overview, Classification, and Declassification*, 6 Apr 22

12. ACCESS TO CLASSIFIED INFORMATION

a. Requirements for Access. Persons shall be allowed access to classified information only if they:

(1) Possess current security clearance eligibility, in accordance with Reference (s). Reference (s) contains detailed guidance on personnel security investigations, adjudications, and accesses;

(2) Have executed an appropriate non-disclosure agreement; and

(3) Have a valid need to know for the information, in order to perform a lawful and authorized governmental function. (Ex 19:40)

DoD Manual 5105.21v3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities,* 19 Oct 20, IC 2, 14 Sep 20

5. THE NEED TO KNOW PRINCIPLE. The primary security principle in safeguarding SCI is access only by those persons with an appropriate clearance, access approval, clearly identified need to know, and appropriate indoctrination. Even when approved for a specific access, the holder is expected to practice need to know in acquiring or disseminating information about the program(s) or project(s) involved. (Ex 18:11)

ENCLOSURE 5 SECURITY INCIDENTS

2. SECURITY INCIDENTS. It is the responsibility of all SCI-indoctrinated personnel to report any security incidents affecting or involving SCI to the appropriate SSO or local SCI security official. Security managers shall ensure all security violations and incidents involving SCI information are reported immediately to the appropriate SSO. An appropriate report shall be prepared and provide sufficient information to explain the incident. Security incidents are categorized as either violations or infractions.

A. Security Violations. A security violation is a compromise of classified information to persons not authorized to receive it or a serious failure to comply with the provisions of security regulations or this Manual and which is likely to result in compromise. A security violation requires investigation.

(1) Violations can result from, but are not limited to, deliberate or accidental exposure of SCI resulting from loss, theft, or capture; recovery by salvage; defection; press leaks or public declarations; release of unauthorized publications; or other unauthorized means.

(2) Loss or exposure of SCI from any cause requires immediate reporting, investigation, and submission of a damage assessment describing the impact on national security.

b. Infractions. An infraction (formerly known as a "practice dangerous to security") is a failure to comply with the provisions of security regulations or this Manual or any other action that causes a potential compromise of classified information.

(1) An infraction requires immediate corrective action but does not require investigation. An infraction does not constitute a security violation but can lead to security violations or compromises if left uncorrected. Examples of infractions include, but are not limited to, a courier carrying classified documents stopping at a public establishment to conduct personal business, or placing burn bags adjacent to unclassified trash containers.

(2) Management officials shall take prompt corrective action on any reported infraction and document the actions taken. (Ex 18:54)

DoDM 5105.21 V1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*, 19 Oct 12, IC 2, Eff 6 Oct 20

ENCLOSURE 2 RESPONSIBILITIES

12. INDIVIDUALS WITH SCI ACCESS. Each individual who has access to SCI shall:

a. Report to proper authorities (SSO, security official, supervisor) any information that could reflect on their trustworthiness or on that of other individuals who have access to SCI, such as, but not limited to things such as:

(1) Violation of security regulations.

b. Immediately report an actual or potential security violation or compromise to an SCI security official (SSO/SSR). In addition, individuals shall report any unauthorized disclosure or exposure of SCI that might reasonably be expected to result in the publication of SCI in the public media such as newspapers, books, television, radio, and internet blogs. (Ex 17:14-15)

DoDM 5200.01V3_AFMAN 16-1404V3, *Information Security Program: Protection of Classified Information,* 12 Apr 22

ENCLOSURE 6 SECURITY INCIDENTS INVOLVING CLASSIFIED INFORMATION

5. SPECIAL CIRCUMSTANCES. Certain types of classified information or specific circumstances require unique handling or consideration of additional reporting requirements.

d. Security Incidents Involving SCI. Actual or potential compromises involving SCI shall be reported to the activity SSO. (Ex 20:100)

DoDM 5200.02_AFMAN 16-1405_AFGM2022-03, *AF Personnel Security Program,* 30 Nov 22

ENCLOSURE 6 REPORTABLE ACTIVITIES

1. Reportable Actions by Others. To ensure the protection of classified information or other information specifically prohibited by law from disclosure, covered individuals shall alert commanders/directors, security managers (assistants), or supervisors to the following reportable activities of other covered individuals that may be of potential security or counterintelligence concern:

a. An unwillingness to comply with rules and regulations or to cooperate with security requirements. (Ex 21:13)

DISCUSSION AND ANALYSIS.

The SAF/IG team interviewed over 240 members, witnesses, and leaders of the 102 IW, as well as Subject Matter Experts (SME) over the course of this investigation. Analysis indicates a number of contributing factors, both direct and indirect, that fostered an environment where an insider threat like A1C Teixeira could remain active over an extended period of time.

Primary Cause of the Unauthorized Disclosure (UD)

Evidence indicates that 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. A discussion of A1C Teixeira's online access and activities, as well as the AF C-InT Hub's capabilities to collect, integrate, and analyze indicators of potential insider threats, are covered in the Classified Annex to this report. 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 ability to commit these unauthorized disclosures.

Direct Contributing Factors

Security Incidents Known, But Not Shared with the SSO

Documentary and sworn testimonial evidence indicate three individuals in A1C Teixeira's supervisory chain had specific and actionable information about as many as four separate instances of his questionable security activity that should have been reported to the 102 ISRG/SSOs. (b) (6), (b) (7)(C) and A1C Teixeira's supervisor, intentionally failed to report multiple security concerns and incidents involving A1C Teixeira to the SSO. By their own admission, these two individuals held a firm belief the SSO might overreact to information concerning A1C Teixeira's activities. They should have informed the SSO in accordance with both DoDM 5200.01 V3, *Information Security Program: Protection of Classified Information*, which states, "Actual or potential compromises involving SCI shall be reported to the activity SSO…"; and DoDM 5105.21 V1, *SCI Administrative Security Manual: Administration of Information and Information Systems Security*, which states each individual who has access to SCI shall "Immediately report an actual or potential security violation or compromise to an SCI security official (SSO/SSR)." (Ex 20:100; Ex 17:15) A1C Teixeira violated both these regulations, as he did not have the requisite need to know the information and persisted in trying to acquire more intelligence information even after being directed to stop. These actions represent at minimum, a potential security violation which should have prompted reporting to the SSO. Had the SSO been informed as required, the SSO would have facilitated restricting systems and facility access and alerted the appropriate authorities, including the DAF Counter Insider-Threat Hub (DAF C-InT Hub) and/or AFOSI. (b) (6), (b) (7)(C), likewise willfully failed to accurately and completely report the same security concerns and incidents involving A1C Teixeira to the SSO. (b) (6), (b) (7)(C)

The four specific instances of A1C Teixeira's activities that should have triggered a notification to the SSO are listed below. Had any of the three members of leadership within the 102 ISRG—(b) (6), (b) (7)(C) —come forward and properly disclosed the information they withheld at the time of the incidents, the length and depth of the unauthorized and unlawful disclosures would likely have been reduced by several months.

Jul/Aug 22: (b) (6), (b) (7)(C) saw A1C Teixeira viewing Top Secret intelligence content on JWICS. Rather than confronting him directly, [redacted] informed A1C Teixeira's supervisor, (b) (6), (b) (7)(C) who did not document the incident. (b) (6), (b) (7)(C) acknowledged the lack of engagement and documentation by (b) (6), (b) (7)(C) but did not follow

[6] [redacted] is currently on T10 orders as an (b) (6), (b) (7)(C), and only spends 20% of [redacted] time overseeing the SSO office. [redacted] performs the majority of SSO duties. (Ex 40:3-4; Ex 43:7-8)

up. (Ex 38:35-36) This was the first of several incidents, taken together with subsequent incidents, not shared with the SSO as required by DoDM 5200.01 V3 and DoDM 5105.21 V1.

15 Sep 22: (b) (6), (b) (7)(C) noticed A1C Teixeira viewing intelligence products and a map on JWICS and saw him writing down information from the map onto a post-it note. The analyst confronted A1C Teixeira about the note and directed him to shred it. However, [redacted] did not verify what was written on the post-it or whether A1C Teixeira actually shredded it. (Ex 47:13-14, 21) That same day, (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) , each wrote separate MFRs to document the incident. (Ex 89; Ex 90) While not documented in either MFR, (b) (6), (b) (7)(C) directed A1C Teixeira "to cease all research where he did not have a need to know." (Ex 44:44; Ex 50:2) This second incident should have been reported to the SSO as required by DoDM 5200.01 V3 and DoDM 5105.21 V1.

25 Oct 22: During a weekly TS-SCI intelligence briefing, A1C Teixeira asked very detailed questions and even attempted to answer questions using suspected TS-SCI information he did not have an apparent need to know. (b) (6), (b) (7)(C) 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 source." (Ex 91) (b) (6), (b) (7)(C) testified [redacted] did not believe A1C Teixeira based on the level of detail and [redacted] knowledge of the information from classified sources. (Ex 38:30) This incident showed A1C Teixeira's continued efforts to obtain TS-SCI information for which he did not have a need to know. (b) (6), (b) (7)(C) again told (b) (6), (b) (7)(C) who ordered Teixeira to "continue to cease and desist" intelligence "deep dives." (Ex 50:2; Ex 91) On 27 Oct 22, (b) (6), (b) (7)(C) documented this incident via another MFR. (Ex 91) Once again, neither (b) (6), (b) (7)(C) reported this third incident to the SSO as required by DoDM 5200.01 V3 and DoDM 5105.21 V1.

30 Jan 23: (b) (6), (b) (7)(C) observed A1C Teixeira viewing Top Secret intelligence content on JWICS again after being previously ordered to cease and desist. [redacted] notified (b) (6), (b) (7)(C) and documented it with another MFR on 4 Feb 23. (Ex 95) This incident reflects A1C Teixeira's continued efforts to seek TS-SCI information and a failure to comply with (b) (6), (b) (7)(C) order to cease and desist. (b) (6), (b) (7)(C) reported three of the four preceding incidents to (b) (6), (b) (7)(C) .[7] (b) (6), (b) (7)(C) told (b) (6), (b) (7)(C) to inform the (b) (6), (b) (7)(C) . (b) (6), (b) (7)(C) confirmed [redacted] was aware of the concerns the same day. [redacted] failed to adequately notify the SSO of the security concerns. According to the SSO, (b) (6), (b) (7)(C) did not share the MFRs with [redacted], but rather, said A1C Teixeira was simply curious and had an honest interest in cross training to the intelligence

[7] 1) 15 Sep 22 post-it note writing (Ex 89; Ex 90); 2) 25 Oct 22 questions/answers during briefing where A1C Teixeira was ordered to cease and desist (Ex 91); and 3) 30 Jan 23 viewing intelligence content on JWICS after being told to stop. (Ex 95)

career field. (Ex 43:172; Ex 44:26) (b) (6), (b) (7)(C) who was present when (b) (6), (b) (7)(C) counseled A1C Teixeira, testified A1C Teixeira denied having any interest working in the intelligence career field. (Ex 44:61-62) (b) (6), (b) (7)(C) failed to meet the reporting requirements directed by DoDM 5200.01 V3 and DoDM 5105.21 V1. The SSO was not given any of the MFRs. This fourth and final incident was not accurately reported to the SSO.

The involvement of (b) (6), (b) (7)(C) in these events, will be discussed in greater detail.

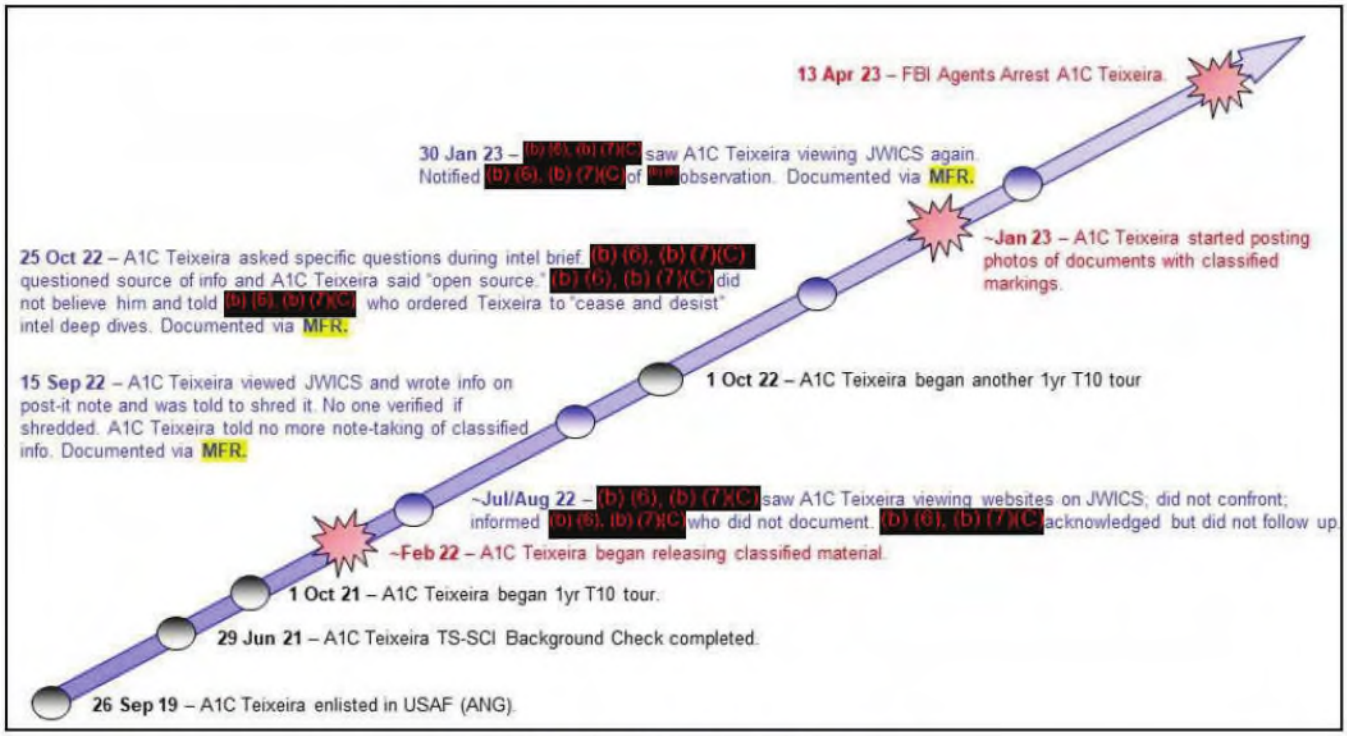

Figure 3: Timeline of Unauthorized Disclosures

"Know Your Why" Initiative Led to Blurred Lines Between System Access and Need to Know

By way of background, need to know is a requirement to make sure an individual, who has the proper security clearance, and properly executed agreements, such as a non-disclosure agreement, also has the required need to know the information in question. It is one of the hallmarks of a compartmented security classification system.

In most cases, the concept of need to know is presented in current guidance 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. (Ex 14:4)

DoD Manual 5105.21v3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities*, 19 Oct 20, IC 2, 14 Sep 20 is more restrictive and tells us in relevant part:

> 5. THE NEED TO KNOW PRINCIPLE. The primary security principle in safeguarding SCI is access only by those persons with an appropriate clearance, access approval, clearly identified need to know, and appropriate indoctrination. Even when approved for a specific access, the holder is expected to practice need to know in acquiring or disseminating information about the program(s) or project(s) involved. (Ex 18:11) (emphasis added)

A "Know Your Why" concept at the 102 ISS, born from 480 ISRW messaging and further emphasized by the (b) (6), (b) (7)(C) and two (b) (6), (b) (7)(C)[8] was designed to encourage Airmen to be "intellectually curious" and more involved in the mission. (Ex 38:22; Ex 60:3; Ex 61:1; Ex 62:3) Implementation of this concept, which allowed IT specialists like A1C Teixeira, to attend TS-SCI intelligence briefings in an effort to help them understand the importance of keeping the classified computer network operating, was poorly implemented in that it provided higher level classified details than necessary to understand the mission. This, in part, created ambiguity with respect to need to know. Whether intended or not, this policy led to a view that being allowed to attend briefings and already having TS-SCI system access to perform duties, meant approval to search and view TS-SCI intelligence products on the classified network. In light of this, the initial instance of A1C Teixeira viewing TS-SCI intelligence before being ordered to stop may not have been a clearly reportable incident. However, when taken together with additional instances of intelligence-seeking behavior after being ordered to stop, the initial instance should have been subsequently reported. A more detailed discussion of conflation of system access and need to know is discussed later in this report as one of the indirect contributing factors to the unauthorized release of national security information.

[8] 480 ISRW holds semi-annual Global Synchronization and Planning Meetings with all subordinate operational units to share best practices, improve overall communication, and continue shaping the future of the enterprise. (Ex 133:1)

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C) (b) (6), (b) (7)(C) is a Title 32 (T32) technician, (b) (6), (b) (7)(C), and was in A1C Teixeira's chain of command as his direct supervisor. (Ex 87:2) (b) (6), (b) (7)(C) During the course of this investigation, (b) (6), (b) (7)(C) security clearance was suspended.

During [redacted] interview, (b) (6), (b) (7)(C) described cyber security as "extremely important" and characterized [redacted] relationship with the SSO, (b) (6), (b) (7)(C) as "friendly."[9] (Ex 42:3) When asked specifically if people in the unit are willing to report infractions or mistakes to the SSO, he quickly responded: "SSO or Cyber Security."[10] (Ex 42:4) (emphasis added) He stated, "No, if there is – if there is a security issue, and this obviously is, you can bring it to either or." (Ex 42:6) He added that Cyber Security works "in tandem" with the SSO office but conceded Cyber Security is not in the same office as the SSO and does not work for the SSO. (Ex 42:4) (b) (6), (b) (7)(C) was incorrect in saying [redacted] could also go to Cyber Security, since DoDM 5200.01 V3 specifically states personnel shall report any security incidents affecting or involving SCI to the appropriate SSO.[11]

(b) (6), (b) (7)(C) *Did Not Agree with the Way the SSO Handled Security Incidents and Believed Reporting Things to the SSO was Discretionary*

There were at least four other occasions where subordinates of (b) (6), (b) (7)(C) had security incidents, and (b) (6), (b) (7)(C) did not agree with the way they were handled by the SSO, (b) (6), (b) (7)(C) Evidence shows (b) (6), (b) (7)(C) sought to keep the information close hold within [redacted] flight. A recurring theme [redacted] espoused was "there is a reluctancy among some to go to the SSO," further explaining: (Ex 42:7)

> [S]ome of my guys…have found themselves reporting something on the right side of the track to then all of a sudden, feel like they are on the wrong side of the track because of the manner in which the Security Office [SSO] can present itself. So, you can quickly say, 'I saw this person doing this thing,' and then, now you are being read your *Miranda* rights….I think there is a reluctancy among some to go to the SSO. (Ex 42:7)

[9] (b) (6), (b) (7)(C) 102 ISS member, countered (b) (6), (b) (7)(C) assertion that [redacted] relationship with the SSO was "friendly," testifying (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) did not get along. [redacted] also countered the assertion that people are reluctant to engage with (b) (6), (b) (7)(C) as (b) (6), (b) (7)(C) alleged, adding [redacted] is comfortable with (b) (6), (b) (7)(C) (Ex 69:1-2)

[10] Witnesses referred to the ISSM and ISSO as "Cyber Security" or the "Cyber Security Office."

[11] DoDM 5200.01, V3, 12 Apr 22, Enclosure 6, para 5d: "Security Incidents Involving SCI. Actual or potential compromises involving SCI shall be reported to the activity SSO…" (Ex 20:100)

Contrary to (b) (6), (b) (7)(C) assertions, as discussed below, the evidence does not support there was a general reluctance among unit members to report matters to the SSO. There is, however, ample evidence indicating (b) (6), (b) (7)(C) was reluctant to bring issues to the SSO or did not think [redacted] should. For example, during [redacted] testimony, (b) (6), (b) (7)(C) first described an incident where one of [redacted] subordinates took a classified password, wrote it down on a post-it note, placed it in their pocket, took it outside of the vault, and dropped it on the floor while getting a snack. (Ex 42:5) A co-worker later found the post-it and turned it in—not to the SSO—but to Cyber Security, a different office. Cyber Security later took it to the SSO. The member in question who dropped the note was (b) (6), (b) (7)(C) [redacted] (b) (6), (b) (7)(C) differentiated this post-it note incident from A1C Teixeira writing down information from a map viewed on JWICS by rationalizing no one actually knew what was written on A1C Teixeira's post-it note and A1C Teixeira assured (b) (6), (b) (7)(C) he had shredded it. (Ex 50:2) (b) (6), (b) (7)(C) commented on this in a statement (b) (6), (b) (7)(C) [redacted]:

> Another ISS member found [the post-it] and brought it to the Cyber Security shop, Cyber Security then brought it to the SSO. This was deemed to be a Security Incident…This member received a Letter of Counseling per my direction…because we knew the exact contents of the note and determined he violated standards based on the evidence. (Ex 50:2)

(b) (6), (b) (7)(C) pointed to this story as an example of how information about a security incident did not necessarily have to go to the SSO, that it could make its way from Cyber Security to the SSO, thus obviating the need to take it directly to the SSO. (Ex 42:6) [redacted] further testified [redacted] instructed Airmen they could bring information about a security issue to *either* the chain of command (to [redacted]) *or* to Cyber Security *or* the SSO. (Ex 42:7) He suggested he had some leeway to decide for [redacted] whether something amounted to a security incident or not:

> [D]on't get me wrong. I would never not report a security incident <u>if I thought one happened</u>, but there is a bit of reluctance in making sure that you are 100 percent on point. It's not a – it's not a two-way conversation. And I get it. Some spots there is a need for a police officer, but it's very black-and-white. But life isn't always 100 percent black-and-white. There is the human factor involved. (Ex 42:8) (emphasis added)

Even though (b) (6), (b) (7)(C) later told investigators [redacted] had an uneasy feeling about A1C Teixeira, and that [redacted] intelligence-seeking behavior was "unhealthy," [redacted] did not report those concerns to the SSO: (Ex 50:3)

> Despite the lack of facts in the [A1C Teixeira] sticky note situation and based on my gut in those moments, I decided to deviate from command culture, and directed him to cease all research where he did not have a need to know. I made myself extremely clear and made sure he acknowledged my message. <u>I felt something was awry</u>, taken as whole with his demeanor, but I did not have any tangible evidence that anything was outside of permissible parameters. I had no tangible evidence he was doing anything illegal, merely

that his desire to obtain information was at a minimum, unhealthy based on my experience. (Ex 50:2) (emphasis added)

(b) (6), (b) (7)(C) testified about a second incident in which one of [redacted] subordinates, (b) (6), (b) (7)(C) [redacted], gave [redacted] administrative permissions to a Special Access Program (SAP) folder on the classified network. According to (b) (6), (b) (7)(C) this "is common, from what I was told."[12] (Ex 42:12) (b) (6), (b) (7)(C) described when (b) (6), (b) (7)(C) actions were discovered, the SSO had concerns [redacted] was an insider threat and (b) (6), (b) (7)(C) was brought into the SSO's office about the situation. Rather than being concerned about getting to the bottom of the security matter, (b) (6), (b) (7)(C) was more concerned (b) (6), (b) (7)(C) might be questioned or read [redacted] rights, and he felt that it could be traumatic for [redacted] Despite this, according to (b) (6), (b) (7)(C) it all worked out and [redacted] was not disciplined at all. (Ex 42:14)

(b) (6), (b) (7)(C) [redacted], was interviewed and asked [redacted] opinion if (b) (6), (b) (7)(C) would come to [redacted] or the SSO if he had an incident, question, or concern regarding a security violation. [redacted] testified [redacted] was not confident (b) (6), (b) (7)(C) would do so, adding that [redacted] believed (b) (6), (b) (7)(C) coaches [redacted] subordinates to not disclose things to Cyber Security or the SSO. (Ex 49:40-41)

(b) (6), (b) (7)(C) pointed to [redacted] concerns with how the (b) (6), (b) (7)(C) incidents were handled as justification for [redacted] reluctance to report A1C Teixeira's issues to [redacted] This demonstrates a pattern of (b) (6), (b) (7)(C) having personal reservations about bringing security concerns to the SSO.

(b) (6), (b) (7)(C) described [redacted] as having a "police officer demeanor" and believed [redacted] had a reputation as a "career crusher." (Ex 42:8) [redacted] was very concerned about the way [redacted] a former Security Forces member (b) (6), (b) (7)(C) [redacted]

While (b) (6), (b) (7)(C) offered these anecdotes as reasons why people were supposedly reluctant to report things to the SSO, witness testimony and AFIA interviews of nearly 200 Airmen do not support this view. (Ex 104:15-16) Witnesses indicated a vast majority of members knew [redacted] understood the importance of reporting incidents, and regularly and routinely self-reported their own mistakes such as accidently taking a smart watch or cell phone into the vault. When asked if [redacted] is unapproachable or a "career crusher," officers and enlisted leaders in the 102 IW did not see it that way. (Ex 52:3; Ex 59:3; Ex 60:3; Ex 61:2; Ex 62:3) Instead, they described [redacted] as "professional and very approachable," "very personable," a helpful resource," and "easily the most knowledgeable and effective SSO in our

[12] According to the Rules of Behavior and Acceptable Use Standards for Air Force Information Technology, this is a prohibited practice and a violation of DAFMAN 17-1301, *Computer Security (COMPUSEC).*

history." (Ex 61:2; Ex 59:3; Ex 60:3) While the (b) (6), (b) (7)(C) , thought (b) (6), (b) (7)(C) was unapproachable, clarified (b) (6), (b) (7)(C) is "no nonsense" and makes sure people know that "the rules are rules." (Ex 64:3)

(b) (6), (b) (7)(C) , testified about a time when another subordinate of (b) (6), (b) (7)(C) , may have improperly given access to an operations crew member without proper authority. (Ex 123:1) (b) (6), (b) (7)(C) explained when (b) (6), (b) (7)(C) learned of it, (b) (6), (b) (7)(C) told (b) (6), (b) (7)(C) viewed it as "responsibility to protect my guys from cybersecurity," or words to that effect. (Ex 45:84) At least two witnesses stated (b) (6), (b) (7)(C) holds the view has to protect subordinates from cybersecurity and this is another example of (b) (6), (b) (7)(C) having personal reservations about bringing issues to the SSO. (Ex 41:23; Ex 45:84)

(b) (6), (b) (7)(C) next testified about another incident involving subordinate, (b) (6), (b) (7)(C) where utilized a retired member's Systems Administrator (Sys-Admin or SYS AD) account and allowed other 102 ISS Sys-Admin personnel to log in under the retired member's account as well. (Ex 42:14) did not address the question of whether that information came to first before it was learned by the SSO. However, (b) (6), (b) (7)(C) testified the incident did not first come to from (b) (6), (b) (7)(C) even though (b) (6), (b) (7)(C) was aware of it:

> IO: [I]s it your understanding that (b) (6), (b) (7)(C) was still [(b) (6), (b) (7)(C)] supervisor at that point?
>
> (b) (6), (b) (7)(C) I believe was, yes.
>
> IO: Is it your understanding that had knowledge of that before your office did?
>
> Yes.
>
> IO: How do you know that?
>
> I believe (b) (6), (b) (7)(C), when was talking to me, had mentioned that to me at one point.[13]
>
> IO: Did you have another conversation with (b) (6), (b) (7)(C) similar to the one you did previously when you found out about the first incident, about that?
>
> I believe I did.

[13] On 26 Apr 23, IG investigators interviewed (b) (6), (b) (7)(C) . confirmed has heard (b) (6), (b) (7)(C) tries to protect people from cyber security and the SSO's office and demonstrates "attitude" and "pushback" when asked about it. (Ex 49:38-42)

IO: How did that go?

[redacted] The usual norm. They didn't think they needed to get us involved.

IO: Is that what [redacted] said?

[redacted] I'm paraphrasing. I'm trying to think back specifically. A lot of times, again, I get the impression that if they go to Cyber Security first that's going to resolve, like reporting.

IO: That's what I'm getting at. Does [redacted] think that if [redacted] goes to IA or to the Cyber Security guys and they can clear it…, the requirement doesn't have to come to you?

[redacted] Yes; correct.

IO: And as we discussed here earlier, that's not the case?

[redacted] That is what sparked that flowchart right there, after [redacted].

IO: Who made this flowchart?

[redacted] [redacted]. (Ex 43:115-116) (emphasis added)

[redacted] displayed a pattern of not reporting incidents within [redacted] flight to proper authorities in order to protect his subordinates. (Ex 45:84)

The flowchart mentioned by [redacted] was created by the then-[redacted] to try to establish a standardized process for responding to security related incidents. It is reproduced in relevant part below and was widely distributed across the group.

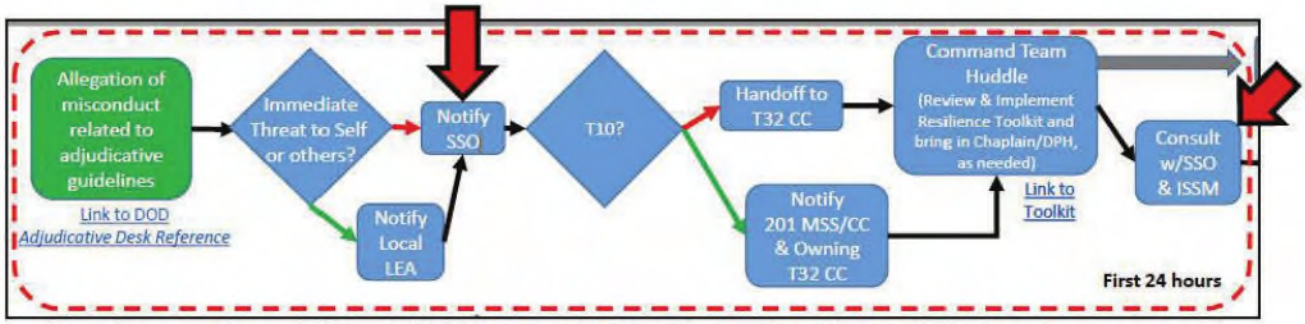

Figure 4: Security Incident Reporting Flowchart (Ex 111:1)

Of note, the (added) red arrows above indicate the requirement to engage with the SSO not once, but twice within the first 24 hours of an allegation of security-related misconduct. There are no avenues around the "Notify SSO" and "Consult w/SSO & ISSM" steps. [redacted]

According to (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) had enough concerns about A1C Teixeira to go to information security to see if they could "do a quick scan" of A1C Teixeira's activities on the classified network, but noted at best a scan like this could only determine logins, not content of material viewed. (Ex: 38:57) [redacted] added, "We were trying to figure out how it would work without him [A1C Teixeira] being present." (Ex 38:57) In this way, (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) went to great lengths to avoid taking the issue to the SSO.

In another instance, (b) (6), (b) (7)(C) showed [redacted] unwillingness to report matters, in an attempt to protect [redacted] subordinates from proper reporting or investigation. (Ex 45:84; Ex 69:1)

(b) (6), (b) (7)(C) [redacted]

(b) (6), (b) (7)(C) [redacted] Rather than addressing the (b) (6), (b) (7)(C) concerns, [redacted] told members of [redacted] unit:

> * Talk to the boss: If it appears that the gossip is getting out of hand, you may need to present the situation to your supervisor. Most bosses want to know about circumstances that are negatively impacting team morale and productivity and will take appropriate steps to rectify the situation – while safeguarding your anonymity. (Ex 99:2)

(b) (6), (b) (7)(C) [redacted] The allegations (b) (6), (b) (7)(C) were ultimately Substantiated. (Ex 69:1)

[14] https://www.syntrio.com/blog/the-negative-impact-of-gossip-in-the-workplace/

(b) (6), (b) (7)(C) continued, on the topic of perceptions about disciplinary response within the unit, by describing the culture of the 102 ISS as "reluctance to discipline even at a verbal level." [redacted] said, "NCOs aren't quite independent or self-sufficient on discipline." Adding, "because the NCOs are not allowed to be independent on discipline, they don't know how to do it. The Flight Chiefs handle discipline." (b) (6), (b) (7)(C) explained (b) (6), (b) (7)(C) has a habit of dealing with personnel matters "within the flight." For instance, [redacted] explained when Quality Assurance (QA) evaluates (b) (6), (b) (7)(C) subordinates, [redacted] accuses QA of "targeting [redacted] Airmen." (Ex 69:2)

Early Warning Information of A1C Teixeira Being a Potential Insider Threat That Should Have Been Reported

(b) (6), (b) (7)(C) served as A1C Teixeira's (b) (6), (b) (7)(C) crew lead (b) (6), (b) (7)(C). During that time, [redacted] described A1C Teixeira as odd and recalled he appeared to have no friends. (b) (6), (b) (7)(C) recalled A1C Teixeira was very interested in guns. (Ex 68:1)

In Mar 22, (b) (6), (b) (7)(C) went to (b) (6), (b) (7)(C) and had a closed-door meeting to express concerns about A1C Teixeira having the potential to be an active shooter. After witnessing hours of A1C Teixeira talking during 12-hour night shifts, (b) (6), (b) (7)(C) felt [redacted] had a good sense of A1C Teixeira's personality. Specifically, [redacted] advised (b) (6), (b) (7)(C) that A1C Teixeira liked to talk a lot about guns; he wanted a machine gun and talked about suppressors. (b) (6), (b) (7)(C) recalled A1C Teixeira wanted to live on a large piece of land so he could "blow stuff up" and talked about explosives, wanted a "no-tech" car, and wanted to live off the grid. In (b) (6), (b) (7)(C) opinion, A1C Teixeira exhibited a fringe thinking perspective. [redacted] testified [redacted] had a "Ted Kaczynski" (a.k.a. "Unabomber") feeling about A1C Teixeira. (Ex 68:1)

The impetus for (b) (6), (b) (7)(C) taking [redacted] concerns about A1C Teixeira to (b) (6), (b) (7)(C) was a discussion (b) (6), (b) (7)(C) had with (b) (6), (b) (7)(C), who heard from people in the 101 IS that A1C Teixeira was denied a gun permit in high school because other students called the police station to report Teixeira wanted to "shoot up the school." (b) (6), (b) (7)(C) testified, "From all our training, this was a red flag, it was tripping all the indicators." (Ex 68:1) (b) (6), (b) (7)(C) went to (b) (6), (b) (7)(C) with the information. [redacted] did not know what (b) (6), (b) (7)(C) did with the information, but A1C Teixeira was moved off [redacted] crew. According to (b) (6), (b) (7)(C) a few weeks later, (b) (6), (b) (7)(C) came back to [redacted] and asked clarifying questions, such as why [redacted] thought A1C Teixeira was an active shooter risk and questioned who told [redacted] the high school story. (Ex 68:1)

About ten months later, around Jan 23, (b) (6), (b) (7)(C) was on a shift rotation where [redacted] worked in (b) (6), (b) (7)(C) office. [redacted] overheard a conversation between (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) who were talking about A1C Teixeira. A1C Teixeira had been late for duty again, which initiated the conversation. (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) also made a vague

reference to A1C Teixeira accessing information without a need to know, and they discussed A1C Teixeira having the potential to be an active shooter. (Ex 68:2) By this account, the issue was still on (b) (6), (b) (7)(C) mind nearly a year after learning of the concerns, yet [redacted] still had not reported it to the SSO or law enforcement. (Ex 43:12)

(b) (6), (b) (7)(C) also testified [redacted] had concerns about A1C Teixeira, which [redacted] had discussed previously with (b) (6), (b) (7)(C) According to (b) (6), (b) (7)(C) A1C Teixeira tried to get a Firearms ID Card (FID) but it was denied because in high school he allegedly "threatened to shoot up the school."[15] (Ex 67:2) (b) (6), (b) (7)(C) took that information to [redacted] supervisor at the time, (b) (6), (b) (7)(C), who remarked, "I bet that's not on his SF-86."[16] (Ex 67:2)

Shortly thereafter, (b) (6), (b) (7)(C) brought the same information to a squadron training meeting, attended by the (b) (6), (b) (7)(C) at the time, (b) (6), (b) (7)(C) [redacted] (Ex 67:2) Upon hearing this information again at the training meeting, (b) (6), (b) (7)(C) recalled (b) (6), (b) (7)(C) responded: "It's not me that's gonna get shot, [redacted] will be first, and then you, [redacted]."[17] (Ex 67:2)

As A1C Teixeira was still new to the unit at that time, (b) (6), (b) (7)(C) was said to have inquired about who A1C Teixeira was. (b) (6), (b) (7)(C) explained A1C Teixeira was the one that had expressed interest and asked questions during (b) (6), (b) (7)(C) intelligence briefings. When asked about the meeting, (b) (6), (b) (7)(C) testified [redacted] remembered parts of the meeting, including A1C Teixeira's fascination with firearms, but claimed [redacted] did not recall discussion about A1C Teixeira having the potential to be an active shooter. (Ex 39:37-38) According to (b) (6), (b) (7)(C) there was no follow-up discussion at the meeting, or afterward, about checking his SF-86, or talking with the SSO or the 102 IW Information Protection Officer (IPO). [redacted] did not go to the SSO or IPO [redacted] as was required under DoDM 5200.01 V3, reasoning [redacted] had notified [redacted] leadership and believed they would act on the information. (Ex 67:2)

(b) (6), (b) (7)(C) also relayed it was known in the unit that there was something "off" about A1C Teixeira. [redacted] recalled a time in 2021, having lunch with (b) (6), (b) (7)(C) [redacted], and other 101 IS personnel. Someone asked about A1C Teixeira, referring to him as "the active

---

[15] Firearms Identification Card (FID): In Massachusetts, permits the purchase, possession, and transportation of non-large-capacity rifles, shotguns, and ammunition. (Ex 120)

[16] SF-86 is a US Office of Personnel Management form, Questionnaire for National Security Positions. It is used in conducting background investigations, reinvestigations, and continuous evaluations of persons under consideration for, or retention of, national security positions as defined in 5 CFR 732, and for individuals requiring eligibility for access to classified information under Executive Order 12968.

[17] (b) (6), (b) (7)(C) [redacted] He used to work in the unit and was well known to some of those in this meeting.

shooter kid," and it was understood among those present they were talking about A1C Teixeira. (Ex 67:2)

After (b) (6), (b) (7)(C) was informed about these concerns with A1C Teixeira having the potential to be an active shooter (as early as Summer 2021), another event occurred which should have prompted (b) (6), (b) (7)(C) to take action and report what [redacted] knew to the proper authorities. In Dec 22, 102 SFS personnel responded to a call about a vehicle parked in the 102 ISRG parking lot that had been left running for a long period of time. (Ex 98:1) The responding officer noticed multiple shooting targets and a large military-style backpack in the rear seat and radioed in for the vehicle's registration. He noted the vehicle belonged to A1C Teixeira, and the Base Defense Operations Center (BDOC) advised A1C Teixeira had 14 legally registered firearms. (Ex 98:1) BDOC contacted A1C Teixeira's unit so he could come outside and speak with the officer, who did not see any visible firearms through the car window, but wanted to remind A1C Teixeira of the "no firearms while on military property" policy. (Ex 98:1)

While waiting for A1C Teixeira to arrive, (b) (6), (b) (7)(C) intervened by approaching the officer, identified himself as A1C Teixeira's supervisor, and wanted to know if "everything was alright?" (Ex 98:1) The officer, (b) (6), (b) (7)(C) told (b) (6), (b) (7)(C) [redacted] wanted to ask A1C Teixeira a few questions about the contents inside his vehicle. When A1C Teixeira came out, (b) (6), (b) (7)(C) told A1C Teixeira that used shooting targets visible in a vehicle could be concerning to Security Forces, and A1C Teixeira said he would remove them from the vehicle when he got home. (b) (6), (b) (7)(C) advised [redacted] was aware A1C Teixeira had over a dozen registered firearms and directly asked A1C Teixeira if he had any firearms inside his vehicle. A1C Teixeira quickly denied this and offered to let (b) (6), (b) (7)(C) search the vehicle. (Ex 98:1-2) (b) (6), (b) (7)(C) did not "feel the need to search the vehicle," so [redacted] declined and A1C Teixeira departed the scene. (Ex 98:2) When (b) (6), (b) (7)(C) returned to BDOC, (b) (6), (b) (7)(C) called [redacted] on the phone. (b) (6), (b) (7)(C) told [redacted] A1C Teixeira did nothing wrong, illegal, or immoral to the point where (b) (6), (b) (7)(C) needed to be involved, and further police action was not warranted. (Ex 98:2) (b) (6), (b) (7)(C) then stated the reason for [redacted] call was that the unit was keeping documentation against A1C Teixeira, and believed something was suspicious about his conduct. (Ex 98:2) (b) (6), (b) (7)(C) told (b) (6), (b) (7)(C) to report anything wrong or suspicious to SFS, and (b) (6), (b) (7)(C) said [redacted] may stop by to fill out a statement. (Ex 98:2) (b) (6), (b) (7)(C) never followed up with SFS and never reported the matter to the SSO. (Ex 98:2)

Between Feb and Mar 23, (b) (6), (b) (7)(C) called (b) (6), (b) (7)(C) into (b) (6), (b) (7)(C) office. (b) (6), (b) (7)(C) was the (b) (6), (b) (7)(C) who was later replaced by (b) (6), (b) (7)(C) With (b) (6), (b) (7)(C) present, (b) (6), (b) (7)(C) asked (b) (6), (b) (7)(C) "Have you heard this story about Teixeira, about him in high school?" (Ex 67:3) (b) (6), (b) (7)(C) said [redacted] had and reminded (b) (6), (b) (7)(C) [redacted] was the one that told him and the squadron leadership about it back in 2021. (Ex 67:3)

Shortly thereafter, (b) (6), (b) (7)(C) for A1C Teixeira and (b) (6), (b) (7)(C), informed (b) (6), (b) (7)(C) that before shift began, (b) (6), (b) (7)(C) met with in (b) (6), (b) (7)(C) office. (b) (6), (b) (7)(C) reportedly told (b) (6), (b) (7)(C) to "keep an eye on" A1C Teixeira, because when (b) (6), (b) (7)(C) told him to stop viewing classified intelligence products, there was a *personality shift* in A1C Teixeira—he seemed like a completely different person—and (b) (6), (b) (7)(C) did not want him to do something drastic. (b) (6), (b) (7)(C) took that to mean (b) (6), (b) (7)(C) was worried A1C Teixeira would bring a gun to work that night and "dumped the issue on a TSgt." (Ex 67:3) When asked if would have handled it differently than (b) (6), (b) (7)(C) responded, "Yes, I would have gone to [(b) (6), (b) (7)(C) [SSO] back in 2021." (Ex 67:3) (b) (6), (b) (7)(C) did not report these concerns to the SSO or law enforcement.

(b) (6), (b) (7)(C) was interviewed on 6 Jun 23 to see if could corroborate (b) (6), (b) (7)(C) account of conversations with (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) testified that in Oct 22, was an (b) (6), (b) (7)(C). confirmed a time (b) (6), (b) (7)(C) directed to come into office, where A1C Teixeira was. (b) (6), (b) (7)(C) did not specifically state or issue a "cease and desist" order per se, but (b) (6), (b) (7)(C) was talking to A1C Teixeira about not looking at classified material he did not have a need to know and stated he could not be looking at classified on JWICS. (Ex 66:1-2) (b) (6), (b) (7)(C) had also been aware of talk about A1C Teixeira being overly interested in JWICS but was not aware of any official direction to A1C Teixeira about it until then. stated it was apparent from (b) (6), (b) (7)(C) conversations that this had been an ongoing issue for A1C Teixeira. Only A1C Teixeira, (b) (6), (b) (7)(C) were present at the meeting. To (b) (6), (b) (7)(C) knowledge, no paperwork was issued to A1C Teixeira as a result. (Ex 66:2)

After A1C Teixeira was dismissed, (b) (6), (b) (7)(C) confirmed (b) (6), (b) (7)(C) told to "keep an eye on him" because was concerned about his "emotional stability." (Ex 66:2) said wanted (b) (6), (b) (7)(C) to be a mentor, wingman, and good NCO to A1C Teixeira. (b) (6), (b) (7)(C) noted how A1C Teixeira looked demoralized and depressed when told him to stop searching intelligence information on JWICS. (b) (6), (b) (7)(C) understood (b) (6), (b) (7)(C) to be concerned about A1C Teixeira being an active shooter threat, although that was not explicitly stated. (b) (6), (b) (7)(C) felt was to keep an eye on A1C Teixeira over (b) (6), (b) (7)(C) concerns "he may shoot up the place." (Ex 66:2)

(b) (6), (b) (7)(C) described A1C Teixeira as out of the ordinary, socially isolated, not tuned into social norms, and very into guns and living off the grid, but said did not personally consider an actual active shooter threat. That said, had heard rumors and whispers of A1C Teixeira being an "active shooter." (Ex 66:2) (b) (6), (b) (7)(C) told (b) (6), (b) (7)(C) to report back to with any concerns or issues. (b) (6), (b) (7)(C) followed-up a week or so later, but (b) (6), (b) (7)(C) did not have anything to report. did not see any specific instances that convinced A1C Teixeira was an active shooter threat. (b) (6), (b) (7)(C) did ask A1C Teixeira

why he was so interested in JWICS and A1C Teixeira responded, "I like knowing things other people don't." (Ex 66:2)

Despite all of these indicators, it was not until after A1C Teixeira's arrest that (b) (6), (b) (7)(C) finally told AFOSI that A1C Teixeira's behavior was comparable to that of an active shooter. AFOSI noted, "Those behaviors, combined with [A1C Teixeira's] interest in firearms and [(b) (6), (b) (7)(C) position as disciplinary figure, caused (b) (6), (b) (7)(C) to become concerned for [redacted] own safety." (Ex 87:2)

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C) made the following unsolicited statement:

> [(b) (6), (b) (7)(C) and I are the ones that did everything right and we're the ones that are going to get in trouble for it. My commander was gone for a week, and when [redacted] comes back, [redacted] laughing, and told me, 'You called it!' (Ex 121)

Two weeks after the FBI arrested A1C Teixeira and interviewed (b) (6), (b) (7)(C) for their investigation, (b) (6), (b) (7)(C) attempted to put A1C Teixeira on the regular work schedule. In a 25 Apr 23 Microsoft Teams Message, (b) (6), (b) (7)(C) informed the (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) of upcoming schedule changes, which included A1C Teixeira returning to day shift. (Ex 129:1) (b) (6), (b) (7)(C) responded incredulously, refused to accept this decision, and asked (b) (6), (b) (7)(C) if [redacted] had anyone else to work that shift. In response, (b) (6), (b) (7)(C) simply remarked, "I do not. It's a 2-person crew now." (Ex 129:3) This exchange, two weeks after a monumental national news event occurring within the unit, is a stark example of (b) (6), (b) (7)(C) lack of situational awareness or appreciation for the gravity of the matter.

On 11 May 23, (b) (6), (b) (7)(C) submitted a 4-page statement with attachments. The full document is included as Exhibit 50. In summary, (b) (6), (b) (7)(C) provided a sworn statement pointing to other unit members besides [redacted] with certain pieces of information about A1C Teixeira's conduct, including (b) (6), (b) (7)(C) [redacted] notes members of the supervisory chain had some knowledge, and the ISSM or ISSO were asked to try to trace Teixeira's online activities. This is consistent with items 5, 6, 7, 11, and 13 of the

[18] (b) (6), (b) (7)(C) later provided "Supplemental Testimony and Submission of Matters" (b) (6), (b) (7)(C) [redacted] on 11 May 23. (Ex 50)

General User Agreement and Acknowledgement of Responsibilities, which requires the indication of actual or possible compromise or file access to be immediately reported to the ISSM, ISSO, or SSO. (Ex 50:8-9) However, the User Agreement is specific to Information Systems access, such as JWICS, and is not authoritative on reporting SCI violations or reportable activities.

As stated during [redacted] interview, (b) (6), (b) (7)(C) is relying on this provision, that the guidance says "or" and not "and," as justification for not telling the SSO about all of A1C Teixeira's questionable behavior with respect to both handling and access to classified information, and (b) (6), (b) (7)(C) proclaimed concerns about A1C Teixeira being an active shooter threat. However, several standards have language that are contrary to the User Agreement. For example, DoDM 5200.01V3-AFMAN 16-1404V3, Enclosure 6, Section 3g states:

> g. All DAF personnel who become aware of any possible security incident involving classified information, regardless of whether it did or could have resulted in actual, potential, or suspected loss or compromise of classified information shall immediately report it to their commander or director, supervisor, and security manager. (Ex 20:99)

Later, in Enclosure 6, Section 5d, it more clearly states:

> d. Security Incidents Involving SCI. Actual or potential compromises involving SCI **shall be reported to the activity SSO** and handled IAW Ref (i) and (bj). (Ex 20:100) (emphasis added)

Also, DoDM 5105.21V3, Enclosure 5, Section 2 states:

> 2. SECURITY INCIDENTS. It is the responsibility of all SCI-indoctrinated personnel to report any security incidents affecting or involving SCI to the appropriate SSO or local SCI security official. Security managers shall ensure all security violations and incidents involving SCI information are reported immediately to the appropriate SSO. An appropriate report shall be prepared and provide sufficient information to explain the incident. (Ex 18:54)

Additionally, DoDM 5105.21V1, Enclosure 2, Sections 12a-b state:

> 12. INDIVIDUALS WITH SCI ACCESS. Each individual who has access to SCI shall:
>
> a. Report to proper authorities (SSO, security official, supervisor) any information that could reflect on their trustworthiness or on that of other individuals who have access to SCI, such as, but not limited to things such as:
>
> (1) Violation of security regulations.

b. Immediately report an actual or potential security violation or compromise to an SCI security official (SSO/SSR). (Ex 17:14-15)

Furthermore, (b) (6), (b) (7)(C) belief the security concerns could be reported to the ISSO are also contrary to what members of the 102 ISRG were briefed in their annual security training, which says, "It is the responsibility of the supervisor, 1st Sgt and Commander to ensure all incidents are reported to the *SSO* within 24 hours." (Ex 122:40) (emphasis added) The training also explains "Your Obligation to Report" stating, "There is no 'picking and choosing' on reporting nor 'over reporting.'…'Everything is considered reportable, always pop by the SSO Office to clarify. Do not lie or minimize, be honest.'" (Ex 122:27)

The evidence and analysis indicate (b) (6), (b) (7)(C) violated policy and procedures by failing to report multiple security and safety concerns involving A1C Teixeira to the SSO. [redacted] was A1C Teixeira's direct supervisor and a Senior NCO within the unit with all the information needed and the requirement to report A1C Teixeira's activities. Had (b) (6), (b) (7)(C) acted as required, A1C Teixeira would likely have been unable to continue to acquire and improperly disclose classified materials over an extended period of time. (b) (6), (b) (7)(C) withheld insider threat information and concerns about A1C Teixeira from the SSO and did not keep [redacted] commander, (b) (6), (b) (7)(C) thoroughly informed.

Two witnesses testified that (b) (6), (b) (7)(C) felt it was more important to protect [redacted] subordinates than report a potential insider threat. (Ex 41:23; Ex 45:84) During [redacted] testimony, (b) (6), (b) (7)(C) contradicted himself in characterizing the threat posed by A1C Teixeira, and [redacted] level of concern about him. It cannot be, on the one hand, that A1C Teixeira was benign and not worth mentioning to the SSO, while at the same time, be a concern necessitating (b) (6), (b) (7)(C) to direct others to keep an eye on him, mention concerns about suspicious activity, and order A1C Teixeira to cease and desist looking at classified information.

(b) (6), (b) (7)(C) looked for ways to dispose of the issues while protecting A1C Teixeira from being subjected to, in [redacted] view, unreasonable suspicions or overreactions by the SSO. Unbeknownst to the SSO or the (b) (6), (b) (7)(C) went to (b) (6), (b) (7)(C) not the SSO) and asked for a scan on A1C Teixeira's classified system activity.[19] [redacted] had enough concerns about A1C Teixeira to have someone try to monitor his classified online activity, but would not alert the one person, the SSO, whose primary duties are to ensure the integrity of the SCI Facility (SCIF) and the national security intelligence it contained. No scan was performed on A1C Teixeira's computer based upon this conversation between (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) (Ex 41:28)

It is also inconsistent to joke about who A1C Teixeira might have shot first in an active shooter scenario, tell 102 SFS [redacted] had suspicions about A1C Teixeira, and then later express [redacted]

[19] A more detailed account of tracking capabilities are contained in the Classified Annex.

concerns to AFOSI about A1C Teixeira being a potential active shooter. (b) (6), (b) (7)(C) stated A1C Teixeira's personality and behavior was comparable to what [redacted] believed an active shooter might be like, and claimed those behaviors, combined with A1C Teixeira's interest in firearms and (b) (6), (b) (7)(C) position as disciplinary figure, caused [redacted] to be concerned for [redacted] own safety. (b) (6), (b) (7)(C) told 102 SFS [redacted] had suspicions about A1C Teixeira, though [redacted] never followed through on reporting those concerns formally to 102 SFS and did not mention these same concerns to the SSO. [redacted] noted a personality shift in A1C Teixeira – that [redacted] seemed like a completely different person and was concerned he might do something drastic. (b) (6), (b) (7)(C) noted A1C Teixeira looked demoralized and depressed when told to stop searching intelligence on JWICS and thought enough of it to have a [redacted] keep an eye on him but did not inform the SSO of these combined warning signs A1C Teixeira may do something drastic. DoDM 5200.02, *Air Force Security Program,* states covered individuals[20] shall report "Any activity that raises doubts as to whether another covered individual's continued national security eligibility is clearly consistent with the interests of national security." (Ex 21:13) Given these statements to AFOSI and others, it is notable [redacted] failed to report them to authorities.

(b) (6), (b) (7)(C) testified (b) (6), (b) (7)(C) talked and shared many concerns about A1C Teixeira and his pattern of behavior, all of the different things that had transpired, developing a pattern of behavior and saying they had some serious concerns about this individual; still, they refused to notify the SSO. (Ex 38:64) (b) (6), (b) (7)(C) claimed [redacted] had no tangible evidence A1C Teixeira was doing anything illegal, but in [redacted] own words, it was "merely that [redacted] desire to obtain information was at a minimum, unhealthy based on my experience." (Ex 50:3)

In consciously deciding to withhold the spectrum of security concerns about A1C Teixeira from the SSO, because [redacted] struggled with concerns about potential outcomes based on past experiences, (b) (6), (b) (7)(C) failed to identify an insider threat to national security. (b) (6), (b) (7)(C) eventually brought [redacted] concerns to both (b) (6), (b) (7)(C) following the 25 Oct incident, but when (b) (6), (b) (7)(C) perceived [redacted] as having "zero concerns," [redacted] did not take the matter to the SSO. (Ex 50:3) Had the SSO been advised of the security and safety concerns regarding A1C Teixeira at that point, officials could have facilitated restricting systems and facility access and alerted appropriate authorities, such as the DAF C-InT Hub and/or AFOSI to neutralize the insider threat, possibly reducing the length and depth of the unauthorized disclosures by several months.

[20] Covered Individuals are all persons who have access to classified information or hold sensitive positions. (Ex 21:11)

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C) (b) (6), (b) (7)(C) is the current (b) (6), (b) (7)(C) and is in T10 status.[22] (Ex 38:3) During the course of this investigation, (b) (6), (b) (7)(C) security clearance was suspended.

(b) (6), (b) (7)(C) is a central figure in this investigation. was the senior ranking member of a small group of leaders who did not report insider threat concerns about A1C Teixeira to the SSO and did not keep commander, (b) (6), (b) (7)(C) thoroughly informed.

On 28 Apr 23, (b) (6), (b) (7)(C) was interviewed at Otis ANGB. acknowledged in role, as the (b) (6), (b) (7)(C) "When I took the seat, I understood that in my role I really didn't even have a need to know to be going into Intel…" (Ex 38:21) However, (b) (6), (b) (7)(C) believed in the notion of having non-intel, IT members receive intelligence briefings to better know how to support the mission. Like predecessor, (b) (6), (b) (7)(C) had the 101 IS provide these briefings weekly and added the prior (b) (6), (b) (7)(C) "encouraged [support Airmen] to be intellectually curious and ask about Ops." (Ex 38:21-22) (b) (6), (b) (7)(C), confirmed (b) (6), (b) (7)(C) decided to keep the intelligence briefing practice in place: "(b) (6), (b) (7)(C) tried to reinvigorate that, just to – again, it was for that connectiveness piece I think, keeping them – you know – understanding why they were supporting us, trying to help that relationship." (Ex 44:18) When asked if anyone expressed reservations about IT maintenance Airmen having access to JWICS, not just for their primary duty of working on systems, but for getting smart on current events and intelligence in the name of "know your why," (b) (6), (b) (7)(C) responded:

> No, sir, not up until Jack Teixeira, and the reason being is there was, quite honestly, I don't think any Airman ever—when I took the seat in , I had never seen any Airman actually exercise that encouragement outside of the current intelligence briefings we were

[21] Per AFI 38-101, *Manpower and Organization,* a squadron (b) (6), (b) (7)(C) oversees daily operations. (b) (6), (b) (7)(C)) (6), (b) (7)(C) . (b) (6), (b) (7)(C) (Ex 109:7)

[22] (b) (6), (b) (7)(C) is currently serving on Title 10 Orders from (b) (6), (b) (7)(C).

> provided by the Operations Groups; however, we did know that the Airman, Jack Teixeira, [5 second pause] had more intellectual curiosity that was far outside the baseline of, you know, I'm just, go talk to this one mission area to see how everything's going or ask them "Why do you use this system?" He was far more curious, and we have documentation on that. (Ex 38:23)

[redacted] clarified when [redacted] referred to JWICS, [redacted] was referring generally to TS-SCI material. (Ex 38:23) When asked about the soundness of that practice—of making Airmen understand the importance of their mission short of violating the tenet of "need to know," (b) (6), (b) (7)(C) quickly adopted that observation as [redacted] own and claimed, (b) (6), (b) (7)(C) [redacted] put together after A1C Teixeira's arrest, to reportedly try to figure out how that could have happened, that was one of [redacted] team's findings. "I would say that [is] 100 percent spot on, Sir. That was one of the things we identified in the [redacted]."[24] (Ex 38:24) This [redacted] was put together between the time of A1C Teixeira's arrest and the IG Team's arrival on 25 Apr 23. (Ex 38:16-17)

(b) (6), (b) (7)(C) continued, pointing to a belief that it was IT maintenance troops being given certain Public Key Infrastructure (PKI) certificates that was the reason A1C Teixeira was able to gain access to classified documents on the secure network, positing and answering [redacted] own theoretical question:

> In reality, do they really need those things to function and be effective as a SYS AD? They don't.[25] So, my recommendation to leadership is going to be strip all the PKIs for SYS ADs pending, you know, CC specific approval. If they deem it necessary for one or for whomever, but our SYS ADs don't need it. (Ex 38:25)

(b) (6), (b) (7)(C) also prefaced [redacted] comments with a statement about A1C Teixeira:

> I can honestly say <u>there was nothing within the indicators of what we observed with Airman Teixeira that told us that he was going to potentially leak classified information.</u> If anything, there were <u>more concerns</u> that he might be an <u>active shooter</u> someday, and we had some concerns with that, but we knew something was off. There was definitely a pattern of behavior. (Ex 38:28) (emphasis added)

---

[24] (b) (6), (b) (7)(C) testified about a [redacted] that was put together after A1C Teixeira's arrest to try to figure out how this series of unauthorized disclosures happened and to see what kind of "counter-measures" could be put in place to "mitigate it from happening again." (Ex 38:11) According to (b) (6), (b) (7)(C) this [redacted] was (b) (6), (b) (7)(C) [redacted] idea. (Ex 38:17) However, when asked, [redacted] testified the [redacted] was not [redacted] idea. [redacted] stated, "I'm not going to take credit for that. I don't know. The team came up with it." (Ex 37:51) When asked, [redacted] confirmed (b) (6), (b) (7)(C) was the one who came to [redacted] and volunteered [redacted] services to try to figure out how the disclosures could have happened. (Ex 37:51)

[25] This is not an accurate statement. According to (b) (6), (b) (7)(C) [redacted] IT professionals do, in fact, require some PKIs to perform their duties. (Ex 49:73)

[redacted] claimed it was very difficult to articulate concerns [redacted] had about A1C Teixeira to leadership and "have it stick," yet as the evidence will show in this section, [redacted] intentionally avoided taking those concerns, whether those concerns were regarding intelligence-seeking behaviors or about the potential for gun violence, to the SSO. (Ex 38:28) [redacted] even stated [redacted] had concerns previously:

> I did fail to tell you some events that originally started to spark, you know, just some concern where I wanted to keep my eyes on Airman Teixeira, the first being—the first time I had concerns that he was too intellectually curious, if you will, about, you know, the current climate and classified information as part of his duties as IMOC. (Ex 38:35) (emphasis added)

In particular, (b) (6), (b) (7)(C) stated nine months before A1C Teixeira's arrest, on or about Jul or Aug 22, [redacted] personally saw A1C Teixeira viewing Top Secret intelligence content on JWICS. Rather than confronting him directly, [redacted] informed (b) (6), (b) (7)(C) A1C Teixeira's supervisor, who did not document the incident. (b) (6), (b) (7)(C) acknowledged this lack of documentation by (b) (6), (b) (7)(C) but did not follow up to make sure it was properly documented. As (b) (6), (b) (7)(C) described it, [redacted] was not as concerned that he was looking at classified information on JWICS as [redacted] was concerned he was neglecting his IT duties. (Ex 38:35-36) [redacted] stated:

> [W]hen I looked over, Airman Teixeira was looking at classified information. I did speak to (b) (6), (b) (7)(C) about that, and I said, "This is not acceptable. It should not interfere with his jobs or his duty; that, that needs to be number one, and "the why," understanding the classified environment, is more of an additive, not a baseline." (Ex 38:35-36)

When asked why [redacted] did not confront A1C Teixeira herself, (b) (6), (b) (7)(C) stated, [redacted] "was in the midst of something else" and was about to "head off to either—there was something pressing." (Ex 38:37) [redacted] then stated a different reason for not taking direct action on the spot, "I just wasn't going to address that. That's more ADCON." (Ex 38:37) When asked for clarification, (b) (6), (b) (7)(C) explained [redacted] had Operational Control (OPCON) over A1C Teixeira, but in this instance, "when it comes to disciplinary actions, I have no dog in that fight." (Ex 38:38) When asked directly which was more concerning to [redacted] that A1C Teixeira was not doing his primary duties, or that he was in an area looking at things he shouldn't be looking at, or both, [redacted] responded:

> It was both, Sir. I didn't see any purpose or need for him at that time to be looking into JWICS and, moreover, when there was an outage occurring, I would have expected him, as an IMOC CFP individual, to be making the outage his primary focal point. (Ex 38:39)

Despite these concerns, [redacted] testified [redacted] did not inform [redacted] operational squadron commander, (b) (6), (b) (7)(C) or the ADCON commander, (b) (6), (b) (7)(C) preferring to have a flight or crew lead address it. (Ex 38:39) [redacted] also did not inform the SSO. As (b) (6), (b) (7)(C)

noted, when the SSO was not initially informed of a previous security incident (unrelated to A1C Teixeira), [redacted] took the initiative to create an incident reporting flowchart:

> Yeah. Tried to handle it at the lowest level, and it's like, no, this is not – if an Airman is late for work, you can handle it at the lowest level. Potential insider threat activity is not handled at the lowest level. That is a security officer/SIO, or if it's not SCI, it's – you know – commander. There's no question. And that was – going back to the culture stuff I was talking about, that was part of the challenge here, right, is trying to get folks to get out of that – we're no longer F-15 maintainers anymore. You're now part of the intel community; we need to act appropriately. (Ex 35:69)

Seven months prior to A1C Teixeira's arrest, on or about 15 Sep 22, (b) (6), (b) (7)(C) described [redacted] too, was aware of the incident in which he was observed by an intelligence analyst writing something down on a post-it note in the SCIF and allegedly attempting to put it into his pocket. (Ex 38:33) [redacted] was aware the analyst confronted A1C Teixeira about the note and directed him to shred it. However, no one ever asked or tried to verify what had been written on the post-it note or whether it was actually ever shredded. (Ex 47:13-14, 21) That same day, (b) (6), (b) (7)(C) each wrote separate MFRs to document the incident. (Ex 89; Ex 90) While not documented in either MFR, according to (b) (6), (b) (7)(C) ordered A1C Teixeira to stop taking notes on classified information. (Ex 44:53) This was the second incident not reported to the SSO as required by DoDM 5200.01 V3 and DoDM 5105.21 V1.

(b) (6), (b) (7)(C) confirmed [redacted] was also present at the intelligence brief on or about 25 Oct 22, then six months prior to A1C Teixeira's arrest, where A1C Teixeira was asking very specific intelligence questions of the briefer. (Ex 38:29) [redacted] testified [redacted] asked him the classification level of the information he was stating, because [redacted] suspected his statements were classified, not unclassified as he claimed, and because the level of detail was not something he would have found in open sources. (Ex 38:30) [redacted] testified [redacted] did not believe him when he claimed the information was not classified and agreed [redacted] had concerns about A1C Teixeira both at that point in time, and prior. (Ex 38:30) Instead of reporting this incident to the SSO, (b) (6), (b) (7)(C) again elected to tell (b) (6), (b) (7)(C) who according to (b) (6), (b) (7)(C) had previously verbally ordered A1C Teixeira to "cease and desist" intelligence "deep dives." (Ex 44:62) On 27 Oct 22, (b) (6), (b) (7)(C) documented this incident via MFR as well. (Ex 91) A1C Teixeira's intelligence-seeking behavior was important enough for (b) (6), (b) (7)(C) to direct (b) (6), (b) (7)(C) to document it with an MFR, but it still was not reported to the SSO.

(b) (6), (b) (7)(C)

When asked about the next incident that made [redacted] suspicious

~~of~~ A1C Teixeira, (b) (6), (b) (7)(C) recalled a conversation [redacted] and A1C Teixeira had about the possibility of him cross training into the intelligence career field:

> (b) (6), (b) (7)(C): When I had observed him being so curious about Intel, it was at that time I thought maybe this wasn't a career field befitting for him. He seemed to have a passion for Intel, so I had a conversation with him about where he was heading because it obviously was something that had interfered with his job. I had asked him if he had considered ever going into Intel. He said [redacted] was previously part of the unit and had steered him towards IT because it's a lucrative career field on the outside.
>
> I had then expressed that it's important that if that's the field of his choice, that that's what he needs to focus in on, and I had mentioned to him that there were other avenues if his passion truly was Intel that he should explore that. He said that was not part of his career path, so I instructed him that he continue to evaluate where he's heading because he needs to focus in on the position that he's in.
>
> IO: And that [was] between the July/August-ish conversation…when you saw him on JWICS, and…the [post it] note [i]n the pocket incident in September?
>
> (b) (6), (b) (7)(C): Yes, Sir. (Ex 38:43)

According to (b) (6), (b) (7)(C) talked about their concerns regarding A1C Teixeira's intelligence-seeking behavior. [redacted] added, (b) (6), (b) (7)(C) told [redacted] had apprised the squadron commander, (b) (6), (b) (7)(C) but according to (b) (6), (b) (7)(C) (b) (6), (b) (7)(C), "seemed aloof" and said that A1C Teixeira had a clearance. (Ex 38:44) Both the (b) (6), (b) (7)(C), witnesses familiar with (b) (6), (b) (7)(C) leadership, did not share (b) (6), (b) (7)(C) characterization of (b) (6), (b) (7)(C) (Ex 60:1; Ex 62:1) The evidence shows (b) (6), (b) (7)(C) took their concerns seriously.

On 5 May 23, the (b) (6), (b) (7)(C), was interviewed. In the wake of A1C Teixeira's arrest [redacted] was suspended (b) (6), (b) (7)(C) and had [redacted] security clearance suspended. (b) (6), (b) (7)(C) testified [redacted] was not aware of the Jul/Aug 22 incident where (b) (6), (b) (7)(C) walked by and saw A1C Teixeira looking at intelligence. (Ex 36:92) [redacted] testified [redacted] was not aware of the 15 Sep 22 incident in which an NCO observed A1C Teixeira writing down information from a classified map or product on JWICS on a post-it note. (Ex 36:93) [redacted] did acknowledge (b) (6), (b) (7)(C) mentioned the intelligence briefing incident on 25 Oct 22 in which A1C Teixeira was asking probing and/or difficult questions and providing specific answers at times during a classified TS-SCI level briefing. (b) (6), (b) (7)(C) recalled it was documented and remembered them using the "cease and desist" phrase. (Ex 36:93-94) [redacted] recalled part of the discussion, including specifically, his understanding the SSO would be involved:

> [T]hey mentioned something to me after the cease and desist where–I can't remember what the content was, where they said, "He's still doing"–I believe it was excessive research or something to that matter, maybe, that they feel–they feel like he's doing excessive research. And that's why [redacted] came to me. [redacted] was like, "I feel like I'm getting the run around." That's when I said, "Alright. Get (b) (6), (b) (7)(C). You guys, you know, document it however you want to document it," that type of thing, but ask–you know, the 201st, [to] get involved. And then I can't remember if it was [redacted] or myself that, you know, getting the SSO involved at that point. (Ex 36:96) (emphasis added)

[redacted] continued, relating [redacted] told (b) (6), (b) (7)(C)

> Get (b) (6), (b) (7)(C), let [redacted] know everything you know. If you feel like you're still not getting where you need to go, come back to me. That's–I'd say that's when probably within the hour, if not shorter, that's when (b) (6), (b) (7)(C) came in. So, assumption is, [redacted] got with (b) (6), (b) (7)(C), [redacted] got what [redacted] needed. (Ex 36:98)

(b) (6), (b) (7)(C) explained (b) (6), (b) (7)(C) came to [redacted] shortly thereafter and discussed the matter. (Ex 36:98) Based on [redacted] testimony, (b) (6), (b) (7)(C) left the conversation with the understanding that the issue, as [redacted] knew it, was being addressed in the right channels:

> IO: And then [redacted] approached you within the hour —
>
> [redacted]: Yes.
>
> IO: And said what?
>
> [redacted]: Kind of the round about the same thing. Teixeira's activities, whatever, it seemed like it–it hasn't improved or whatever–I forget what the nature he actually said, but [redacted] will–[redacted] would like to elevate to the 201st [MSS] and get the SSO involved. And I said, "That's exactly what I would do." (Ex 36:99) (emphasis added)

When asked about the timing of [redacted] discussions with (b) (6), (b) (7)(C) and with (b) (6), (b) (7)(C) clarified: "[T]his and the discussion with myself and [redacted] all happened on the same day." (Ex 36:99)

(b) (6), (b) (7)(C) elaborated:

> [T]hat's when within the hour, (b) (6), (b) (7)(C) was–we're in the breezeway, out here in the hallway. [redacted] said, "I got something for you." We came into my office right here. Said essentially the same thing. Sounds like Teixeira's either, you know, he's still doing it. Maybe he's just not getting it. I forget what the exact verbiage was. [redacted] would like to elevate it to the 201st [MSS] level and maybe get the SSO involved. I said "No, that's exactly what I would do if I were in your shoes." It sounded like it was dealt a path. [sic] And then going back to it, my assumption was, like, that SSO thing was going to happen immediately. It was more of, again–it was fine, like, you do it tied to an adjudicated

standard. It's maybe not, maybe, but however, at least getting an SSO involved, right? (Ex 36:108) (emphasis added)

(b) (6), (b) (7)(C) testified was never provided copies of the MFRs written on A1C Teixeira discussed previously. (Ex 36:123)

(b) (6), (b) (7)(C) was asked if A1C Teixeira violating a direct order to stop looking at intelligence materials made the issue more significant in mind and if that was a concern, when thinking about intelligence-seeking behavior. confirmed it was, and when asked if left conversation with (b) (6), (b) (7)(C) with the understanding that (b) (6), (b) (7)(C) was going to the SSO, indicated that was understanding. (Ex 36:108-109) (b) (6), (b) (7)(C) when asked, did not believe the (b) (6), (b) (7)(C) at the time, (b) (6), (b) (7)(C) had any knowledge of these concerns with A1C Teixeira. (Ex 36:114)

(b) (6), (b) (7)(C) further testified was not ever made aware of the Dec/Jan 23 incident when A1C Teixeira's vehicle was found running in the parking lot by Security Forces with used paper shooting targets and a bag, visible in the back seat—an event (b) (6), (b) (7)(C) responded to and knew about. (Ex 36:106)

(b) (6), (b) (7)(C) stated had not heard about and was surprised to learn that (b) (6), (b) (7)(C) went to (b) (6), (b) (7)(C) after the 25 Oct 22 incident, asking for a scan on A1C Teixeira's classified system activity. deduced from this, (b) (6), (b) (7)(C) must have had concerns about A1C Teixeira, but (b) (6), (b) (7)(C) felt those concerns should have been brought to the SSO's attention. (Ex 36:115)

(b) (6), (b) (7)(C) when asked if (b) (6), (b) (7)(C) mentioned these concerns about A1C Teixeira to anyone else, denied doing so.[26] (Ex 38:45) When asked to explain that, reasoned felt it was hearsay:

> (b) (6), (b) (7)(C): [B]ecause it was hearsay, I mean—when I looked through the training, and I looked through all the different forms of reporting, it seemed as though a[n]area, except for in the caption of "When in Doubt, Ask the SSO," but because it wasn't something that was *seen* by (b) (6), (b) (7)(C) or *seen* by (b) (6), (b) (7)(C), it felt as though it was a grey area.[27] (emphasis added)

[26] (b) (6), (b) (7)(C) would later acknowledge (b) (6), (b) (7)(C) did take the issue of A1C Teixeira to the Information Security shop, (b) (6), (b) (7)(C) to try to get to run a scan of A1C Teixeira's cyber activities. (Ex 38:57) Neither (b) (6), (b) (7)(C) nor the SSO was aware if this.

[27] SSO SCI Annual Refresher Training: "When in doubt ask. It is a violation if you fail to do so and you will be held responsible." (slide 9) "Your accesses will allow you to work/visit the SCIF's [sic] on Otis unescorted. This does not validate your need to know to all projects, caveats, or computer systems. When in doubt…ask!!!!!" (slide 8). (Ex 122:8-9)

IO: Okay. But it was seen by (b) (6), (b) (7)(C), and was there and available, right? Could that have been verified directly with ? In other words, there was a direct witness. The information, you know, didn't sort of come around through hearsay…there was still a direct witness to it; isn't that right?

(b) (6), (b) (7)(C): Yes, Sir.

IO: Okay. Did you think the SSO should have been informed of that?

(b) (6), (b) (7)(C): I will say that part of our calculus when we were talking about the incident, talking about the fact that it was hearsay, discussing that, you know, we didn't see the event ourselves, the Airman [Teixeira] stated that he shredded, they made a misstep or what have you, it was in their pocket and then they shredded it, we were trying to figure out should the SSO be notified. One of the things that did come up in the calculus when we were talking about the event was the SSO has had the tendency of going zero to 100 before in terms of reporting--and so the concern was without having anything substantial, the concern was that if it truly was shredded and didn't leave the building, that we could be potentially opening up a powder keg if it had been reported without substantiation. (emphasis added)

IO: And did you share that concern?

(b) (6), (b) (7)(C): With whom?

IO: Was that (b) (6), (b) (7)(C) concern, your concern, or both of yours?

(b) (6), (b) (7)(C): It was all three of our concerns.[28] (Ex 38:45-47)

(b) (6), (b) (7)(C) admitted decided not to tell the SSO and described thought process for not sharing the information had about A1C Teixeira's questionable conduct to him. For example, was asked, if a concern was in a grey area, as mentioned, who was supposed to be consulted? (Ex 38:47) had copies of training slides with and after a 15 second pause, replied:

Well, the one slide here indicates the SSO, but Sir, I think I would be remiss if I didn't note the fact that in our discussion, because we had a very lengthy behind-door discussion--this wasn't a light decision that was made. (b) (6), (b) (7)(C) brought with experience where the SSO has "Mirandized people" before and/or accused them before, of things that were unsubstantiated, that created a lot of fear and a lot of concern. It's also a very uninviting environment when the SSO (b) (6), (b) (7)(C) . I have also worked with this individual when (b) (6), (b) (7)(C) was the (b) (6), (b) (7)(C)

[28] (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C) for Security Forces. I have been known to see [redacted] talk [redacted] way out of just about everything. So, when it comes to trust level with the SSO, I did not trust [redacted].

...

And my concern was at the time knowing what I know about [redacted], hearing how [redacted] reacted before in situations where there was a lot more fidelity and tangible circumstances to the situation, this I was concerned that one, we'd been encouraging people to be intellectually curious. The individual [A1C Teixeira] said they shredded the piece of paper. So, there was no loss or compromise. It struck us as odd, but there was no concern that classified left the facility. The main concern was that this airman is too focused on operations and not on his primary [job]. (Ex 38:48) (emphasis added)

When pressed as to whether [redacted] had any knowledge that A1C Teixeira actually shredded the post-it or only claimed he had done so, [redacted] conceded it was never verified that he ever actually destroyed it:

IO: So, do you think we should trust him [Teixeira] at his word?

(b) (6), (b) (7)(C): [five second pause] I can't answer that question because at that time, I'm not sure what my --

IO: You were listing that as justification for not reporting it to the SSO, that there was no release; that he had shredded it, and my question to you was, "Was there any verification that he actually shredded it, or just that he said he shredded it?"

W: That would be (b) (6), (b) (7)(C) who, during [redacted] questioning of [redacted], [redacted] is the one who had approached [redacted]. [redacted] would have--we did not validate it, no, Sir…. (Ex 38:49)

When asked if [redacted] was aware of any rules allowing supervisors or commanders to mitigate, or decide on their own, what information should be presented to the SSO, (b) (6), (b) (7)(C) responded, "I don't know that, Sir." (Ex 38:50-51)

(b) (6), (b) (7)(C) personally witnessed and reported to (b) (6), (b) (7)(C) that A1C Teixeira looked at JWICS without a need to know. [redacted] also witnessed him ask questions and state information during briefings, which by (b) (6), (b) (7)(C) own estimation, appeared to have been derived from classified materials, actions [redacted] called "concerning." (Ex 38:39) [redacted] was asked if [redacted] felt those pieces of information were enough for [redacted] to bring them to the SSO's attention. (Ex 38:52) [redacted] responded, "*I* wanted to make sure that we had enough substantiation to say something's not right with this Airman. *I* wanted to get something more quantifiable." (Ex 38:52) (emphasis added) At that point, (b) (6), (b) (7)(C) related how [redacted] instead went to a Security Manager and to the Information Assurance (IA) office to see if [redacted] could determine A1C Teixeira's login activity, to see if it was anything that was, in [redacted] view, "excessive." (Ex 38:53)

(b) (6), (b) (7)(C) reasoned [redacted] did not take these concerns to the SSO, opting instead to see what [redacted] could learn about his classified network log in habits, because a Security Manager is, in [redacted] words, "within the peer-to-peer reporting guide for concerns on insider threat." (Ex 38:53) Despite these concerns, [redacted] added there was pushback on this request to review A1C Teixeira's intelligence viewing activities and stated, "I wasn't able to identify where that line is between intellectually curious and too much, to the point where we were told that, you know, it's a non-issue." (Ex 38:54) (b) (6), (b) (7)(C) went to great lengths to try to dispose of the issues raising concerns about A1C Teixeira and to keep the concerns about A1C Teixeira away from the SSO.

When questioned further about (b) (6), (b) (7)(C) taking the concerns about A1C Teixeira to the Information Assurance Office and Cyber Security instead of the SSO, [redacted] testified [redacted] had a conversation with (b) (6), (b) (7)(C) and claims he questioned, "Who are we to tell somebody they can't look at something?" (Ex 38:59) (b) (6), (b) (7)(C) confirmed this by stating, "…once you grant PKIs, you can essentially see anything you want. Like it doesn't lock it down to need to know…At the time, I didn't see that he was doing anything wrong. He was just curious looking at Intel." (Ex 41:31, 40-41) (b) (6), (b) (7)(C) assessment of A1C Teixeira's need to know was incorrect. PKIs, or access does not obviate the requirement to have a valid need to know. When asked if anyone answered the question regarding whether they could tell A1C Teixeira what he could and could not access on JWICS, (b) (6), (b) (7)(C) stated:

> [redacted]: I was in a pickle, to be honest, Sir, because I didn't know how to respond to that. There was a way that he spun it when he talked about, you know, the research that [redacted] had done to look at classified just for the perspective.[29]
>
> IO: Okay. So, [redacted] was looking, and that's really a, "other kids are doing it too" defense, right? Does that necessarily hold a lot of water, when we think about the conversation we had earlier about access and need to know? How does the fact that other people do it also, obviate the need to make sure that someone has a need to know?
>
> [redacted]: It doesn't, Sir. [six second pause] The thing I find most difficult about all of this now is the hindsight bias because when you compile everything on paper, it looks very cut and dry, but being in it and going through it was much different. (Ex 38:60)

(b) (6), (b) (7)(C) ultimately decided [redacted] did not feel [redacted] had enough information about A1C Teixeira's activities, despite multiple data points over a period of months, which [redacted] referenced as a concern of insider threat, to share what [redacted] had with the SSO. (Ex 38:65, 69) [redacted] believed there was not enough to warrant telling the SSO, or to be able to "quantifiably articulate and show that this [A1C Teixeira's conduct] is beyond the baseline of what was promoted as a culture of curiosity when it came to the mission." (Ex 38:54) In so doing, [redacted] took it upon

[29] (b) (6), (b) (7)(C)

and assumed the risk of deciding what questionable conduct should or should not be reported to the SSO.

(b) (6), (b) (7)(C) was asked specifically, if there needs to be a *perfect* case before taking it to the SSO, or if there was simply a requirement to take it to the SSO. responded by quickly pointing to examples had heard about from (b) (6), (b) (7)(C) about people being "Mirandized" (reminded and advised of their rights) by the SSO, (b) (6), (b) (7)(C) (Ex 38:48) claimed, "that has really driven a lot of anxiety within our members." (Ex 38:54) In support of this line of reasoning, (b) (6), (b) (7)(C) noted a different member wrote a computer password on a post-it note inside the SCIF and lost it outside the SCIF. He was questioned by the SSO and given a rights advisement. This was the same example given by (b) (6), (b) (7)(C) pointed to another security incident when the SSO questioned another member, (b) (6), (b) (7)(C) who was reminded of rights.[30] This incident was likewise mentioned by (b) (6), (b) (7)(C) inaccurately claimed (b) (6), (b) (7)(C) "was doing everything well within right and was almost pegged as an insider threat." (Ex 38:54) Similarly, (b) (6), (b) (7)(C) also later mischaracterized what (b) (6), (b) (7)(C) did as "accessed something by accident." (Ex 38:61) When pressed about whether or not had first-hand knowledge of the facts in those cases, conceded, "(b) (6), (b) (7)(C) informed me of that. I was not there so I can't speak to the particulars of it." (Ex 38:61)

While (b) (6), (b) (7)(C) may have had reservations about interacting with or taking security concerns to the SSO, as discussed, that concern does not appear to be widely held by the more than 200 members of the 102 IW the IG inspection and investigation team interviewed who found (b) (6), (b) (7)(C) to be generally approachable. (Ex 104:15-16) The people held up as examples of the SSO supposedly overreacting to by simply questioning them and advising them of their rights, do not provide a rational justification for not reporting matters about A1C Teixeira to the SSO. feared A1C Teixeira may have been viewed as a potential insider threat, which as it turned out, is exactly what he was. (Ex 38:54) In consciously deciding to withhold security concerns about A1C Teixeira from the SSO because struggled to satisfy own misgivings about potential outcomes, (b) (6), (b) (7)(C) failed to alert the SSO and in turn, AFOSI of a potential insider threat to national security.

Failing to recognize this, (b) (6), (b) (7)(C) continued to state belief that withholding this information was justified:

> (b) (6), (b) (7)(C): So, we, as a squadron, and (b) (6), (b) (7)(C), in particular, because supervised those individuals (b) (6), (b) (7)(C) when those events occurred, was very gun shy and very concerned about how we proceeded and wanted to ensure we had the right information before we went to the SSO, and it was unanimously agreed that if we didn't have it, the potential and likelihood of it getting blown up could be extreme. (emphasis added)

[30] This refers to (b) (6), (b) (7)(C) using a retired member's Sys-Admin account.

IO: So, it's that fear of the SSO's over-reaction that drove the decision. You were the senior person in that group, right? You said it was a unanimous decision, but it's not--I mean, it's not really a democracy, it's not a vote. You were the senior person in that group, and you were all in agreement, you included, that it was a conscious decision not to go to the SSO.

(b) (6), (b) (7)(C): I was the senior person in that group, Sir, but at that point, my commander, who is my supervisor, knew and so did the (b) (6), (b) (7)(C). (Ex 38:55)

(b) (6), (b) (7)(C) went on, claiming both (b) (6), (b) (7)(C) "were apprised of everything that happened," but when pressed, started to re-tell assertions that it was (b) (6), (b) (7)(C) not who told (b) (6), (b) (7)(C) about the first event. also stated talked to (b) (6), (b) (7)(C) after the "post-it event." (Ex 38:56) testified (b) (6), (b) (7)(C) when advised of A1C Teixeira's activities, said A1C Teixeira was simply "a dumb Airman doing dumb things." (Ex 38:56) Later in testimony, however, stated that talked with (b) (6), (b) (7)(C) directly after the running vehicle with shooting targets in the back seat incident, and described reaction as: "When I talked to eyebrows had like-- like 'Yeah, these kids, it's more than just a dumb airman.'" (Ex 38:65-66) testified (b) (6), (b) (7)(C) eventually informed the SSO. A complete discussion of exactly what (b) (6), (b) (7)(C) shared will be covered in depth in a subsequent section of this report examining (b) (6), (b) (7)(C) conduct.

(b) (6), (b) (7)(C) indicated it was the Dec 22 event, three months prior to his arrest, where A1C Teixeira's truck was discovered running in the parking lot, unattended, with shooting targets and a bag in the back seat, that finally convinced there was something wrong with A1C Teixeira:

At that time (b) (6), (b) (7)(C) said that--we had talked--<u>there was [sic] too many things. There was a pattern of behavior</u>, and it was put in front of--sorry, even ranks are eluding me now. (b) (6), (b) (7)(C) --<u>all of the different things that had transpired now like developing the pattern of behavior and saying we have some serious concerns about this individual.</u>

…

Now, like the gun stuff. Like there was some concerns that <u>there's something seriously not right about this individual</u>. (Ex 38:64-65) (emphasis added)

Despite harboring these concerns about A1C Teixeira being both a possible security risk, and, in mind, a potential active shooter, (b) (6), (b) (7)(C) did not come forward and report the information to the SSO.

(b) (6), (b) (7)(C) was asked if witnessed anything regarding (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) discussions about A1C Teixeira. testified about a time when was in (b) (6), (b) (7)(C) office, along with (b) (6), (b) (7)(C). (Ex 44:86, 94) Although (b) (6), (b) (7)(C) did not recall the specific details, remembered the discussion was

security related. (Ex 44:94, 97) During that meeting (b) (6), (b) (7)(C) called (b) (6), (b) (7)(C) . (Ex 44:86) thought (b) (6), (b) (7)(C) asked what should do in a specific instance, maybe saying the words, "I have this Airman who did this. What are your thoughts?" (Ex 44:87) When asked why thought (b) (6), (b) (7)(C) would have called (b) (6), (b) (7)(C) , instead of the actual SSO, about this situation, responded, "I don't know. Maybe felt more comfortable." (Ex 44:96)

In reviewing the testimony, (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) related similar views, particularly with respect to (b) (6), (b) (7)(C) (Ex 42:8-10, Ex 38:54-55) On 25 May 23, the (b) (6), (b) (7)(C) , contacted IG investigators. was interviewed previously and instructed not to disclose the questions or answers in the interview and to advise IG if anyone approached or asked about the content of testimony. (b) (6), (b) (7)(C) advised that at approximately 0800 on 22 May 23, (b) (6), (b) (7)(C) entered office, and stated had a conversation with (b) (6), (b) (7)(C) in which:

> stated (b) (6), (b) (7)(C) collaborated their stories prior to their interviews with the IG team. Specifically, the reason they did not report the incident to the SSO was due to (b) (6), (b) (7)(C) not being approachable. (Ex 51)

This indicates a conscious effort by (b) (6), (b) (7)(C) to plan their testimonies in advance of this IG investigation to try to manipulate the investigation and mitigate their own culpability. This information appears to be credible insomuch as (b) (6), (b) (7)(C) was not privy to (b) (6), (b) (7)(C) actual testimony. Without this knowledge, was able to accurately describe how these two members actually testified. This information was unsolicited and appears to be reliable.

The evidence indicates (b) (6), (b) (7)(C) willfully violated policy and procedures by failing to report multiple security and safety concerns involving A1C Teixeira and was the highest-ranking officer with more than enough information to meet the requirement to notify proper authorities, especially the SSO. After the 25 Oct 22 incident, actions enabled A1C Teixeira to continue to acquire and improperly disclose classified materials for another six months until A1C Teixeira's arrest in Apr 23. was the senior ranking officer who intentionally failed to report classic insider threat information and concerns about A1C Teixeira to the SSO and did not keep commander, (b) (6), (b) (7)(C) adequately informed.

(b) (6), (b) (7)(C) admitted was not aware of any rules allowing supervisors or commanders to mitigate, or decide on their own, what information should be presented to the SSO. decided to try to handle these incidents in house without reporting them to the , whom and (b) (6), (b) (7)(C) considered overbearing. They were more concerned about someone being unnecessarily advised of their rights, than about the possibility of an insider threat. In doing so, circumvented notification requirements to those best suited to stop A1C Teixeira from acquiring additional classified documents and products.

(b) (6), (b) (7)(C) contradicted [redacted] in characterizing this threat and [redacted] level of concern about it. (b) (6), (b) (7)(C) claimed [redacted] wanted to keep an eye on A1C Teixeira, and felt he lied to [redacted] about the source of classified information he was referencing in a TS-SCI briefing. Yet [redacted] believed his claims that he shredded the post-it note he wrote classified information on. [redacted] reticence toward the SSO went so far, [redacted] was willing to call (b) (6), (b) (7)(C) to ask for advice on what to do, instead of informing (b) (6), (b) (7)(C) [redacted] claimed the information [redacted] had was "hearsay," despite the fact [redacted] personally witnessed two of the four incidents, and there were other witnesses with first-hand knowledge. (b) (6), (b) (7)(C) admitted being trained, "When in Doubt, Ask the SSO," yet [redacted] failed to do so. Finally, [redacted] was most senior among those who were aware of four separate security incidents regarding A1C Teixeira and believed he represented a potential active shooter threat but failed to report those concerns.

Had (b) (6), (b) (7)(C) acted prudently and appropriately under the circumstances and the SSO been timely and accurately advised of the security and safety concerns regarding A1C Teixeira, the SSO could have facilitated restricting systems and facility access. Additionally, the SSO could have alerted appropriate authorities, such as the DAF C-InT Hub and AFOSI, to neutralize the insider threat, possibly reducing the length and depth of the unauthorized disclosures by several months.

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C) (b) (6), (b) (7)(C) serving in T10 status.[31] [redacted] Shortly after A1C Teixeira's arrest, [redacted] security clearance was suspended.

(b) (6), (b) (7)(C) had an ongoing discussion with [redacted] regarding A1C Teixeira, and understood [redacted] would explore the opportunity of detailing A1C Teixeira to the 101 IS or the 102d Operations Support Squadron (102 OSS) if that was something he wanted to pursue. (Ex 38:57) According to (b) (6), (b) (7)(C) at one point, learning of some of A1C Teixeira's behaviors, [redacted] characterized him as just "a dumb Airman doing dumb Airman things." (Ex 38:56)

In [redacted] supplemental testimony, (b) (6), (b) (7)(C) stated [redacted] expressed [redacted] concerns with A1C Teixeira's "intel gathering zealousness" to [redacted] as early as Oct 22, six months prior to his arrest, when [redacted] coordinated disciplinary actions with [redacted] for A1C Teixeira's

[31] (b) (6), (b) (7)(C) [redacted]

Fitness Assessment failure. (Ex 50:3) According to (b) (6), (b) (7)(C) had "no apparent appetite" to address [redacted] concerns because A1C Teixeira had the appropriate clearances. (Ex 50:3) Then in Jan 23, three months prior to A1C Teixeira's arrest, (b) (6), (b) (7)(C) again stated [redacted] raised [redacted] concerns about A1C Teixeira's "excessive research efforts" to (b) (6), (b) (7)(C) when [redacted] discussed disciplinary actions with (b) (6), (b) (7)(C) for A1C Teixeira's failure to report to work on New Year's Day. (Ex 50:3) (b) (6), (b) (7)(C) perceived (b) (6), (b) (7)(C) as having "zero concerns" and recalled [redacted] referred to A1C Teixeira as "just a dumb Airman." (Ex 50:3)

Following the 30 Jan 23 incident where (b) (6), (b) (7)(C) observed A1C Teixeira viewing intelligence content on JWICS again after being previously ordered to cease and desist, (b) (6), (b) (7)(C) notified (b) (6), (b) (7)(C) of the incident via a Microsoft Teams message. (Ex 44:78) (b) (6), (b) (7)(C) then informed the (b) (6), (b) (7)(C) . (Ex 36:107) (b) (6), (b) (7)(C) stated (b) (6), (b) (7)(C) felt [redacted] was not getting support from (b) (6), (b) (7)(C) or (b) (6), (b) (7)(C) so (b) (6), (b) (7)(C) directed (b) (6), (b) (7)(C) to get with (b) (6), (b) (7)(C) again and give him everything. (Ex 36:107) (b) (6), (b) (7)(C) told (b) (6), (b) (7)(C) if [redacted] still felt like [redacted] was not getting anywhere, to then come back to (b) (6), (b) (7)(C) and [redacted] would personally address it with (b) (6), (b) (7)(C) (Ex 36:107)

Within an hour of the discussion between (b) (6), (b) (7)(C) , (b) (6), (b) (7)(C) came to speak to (b) (6), (b) (7)(C) and had a discussion where (b) (6), (b) (7)(C) understood (b) (6), (b) (7)(C) would take the matter to the (b) (6), (b) (6), (b) (7)(C) and that SSO notification would happen "immediately." (Ex 36:108)

(b) (6), (b) (7)(C) asked (b) (6), (b) (7)(C) to provide [redacted] the three MFRs [redacted] had written on A1C Teixeira to include: 1) the 15 Sep 22 post-it note writing; 2) the 25 Oct 22 questions/ answers during briefing where he was ordered to continue to cease and desist; and 3) the 30 Jan 23 viewing intelligence content on JWICS after being told to stop. [redacted] sent them to (b) (6), (b) (7)(C) via a Teams message on 4 Feb 23. (Ex 102:1-2)

While (b) (6), (b) (7)(C) did visit the (b) (6), (b) (7)(C) did not relay the information about A1C Teixeira as a security concern and failed to show (b) (6), (b) (7)(C) the MFRs documenting A1C Teixeira's conduct. (Ex 40:33; Ex 43:172-174) (b) (6), (b) (7)(C) described the encounter as follows:

> [(b) (6), (b) (7)(C) came in and [redacted] was--[redacted] was concerned more of "hey, this seems interesting. They came to me and told me all of this." But [redacted] was also going with the knowledge of how they--how the ISS has a tendency--and the personalities involved don't always do the right thing in regards to like reporting or identifying anything. And the fact that they had gone through Cyber Security and then avoided us to go see (b) (6), (b) (7)(C) [(b) (6), (b) (7)(C) was like "hey, they're up to it again." They're doing something that they're not reporting so I'm coming to let you know, "hey, they're kind of like doing this but they don't have anything tangible to give me or to look at in regards to anything, not even like the LOC for the fitness or whatever the case might be. (b) (6), (b) (7)(C) said that I'm

> going on vacation so I gave them [(b) (6), (b) (7)(C) until I get back to give me every single detail or piece of paper, MFR, LOC, whatever the case might be; [redacted] came back, got an LOC for fitness I believe that's what it was. And I believe that at that point in time there was nothing else given. (b) (6), (b) (7)(C) talked with him [A1C Teixeira] for, that maybe he was an inquisitive kid, and felt that there wasn't anything devious going on at that point. (Ex 43:173) (emphasis added)

(b) (6), (b) (7)(C) followed up with (b) (6), (b) (7)(C) when (b) (6), (b) (7)(C) returned from leave to see what documentation they had on A1C Teixeira, and the only thing (b) (6), (b) (7)(C) told [redacted] about was the 27 Oct 22 LOC for A1C Teixeira's Fitness Assessment failure. (Ex 43:177) Even though (b) (6), (b) (7)(C) had the three MFRs from (b) (6), (b) (7)(C) at this point, for some reason [redacted] did not provide them to (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C), recalled (b) (6), (b) (7)(C) explaining the situation as A1C Teixeira was wasting his time or not doing his job, not that A1C Teixeira was doing anything "nefarious." (Ex 40:34) (b) (6), (b) (7)(C) recalled (b) (6), (b) (7)(C) stopping by the office to get (b) (6), (b) (7)(C) opinion and not necessarily to report an incident:

> So, at the end of a duty day, [redacted] approached (b) (6), (b) (7)(C) to get [redacted] opinion. I happened to be leaving. I was getting ready to change, so I sat by. And (b) (6), (b) (7)(C) was a former SSO as well as SSOIC of the same as that shop. So, [redacted] asked us, you know--I don't know exactly who his supervisor was. I think it was [redacted]. He said, "Hey, his supervisor, you know, had seen him on JWICS like reading, you know, essentially classified news, you know, what do you guys think of this?" And, you know, we [(b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) were like, "Well, is he trying to push for additional accesses? Is he trying to see things that he doesn't have access to?" You know, and – and you know, he said "No." You know, and then we asked him – he said to us, "I think he's just trying to cross-train eventually." Then we were like, "Okay, yeah." And that was the end of that interaction on [redacted]. (Ex 40:33)

(b) (6), (b) (7)(C) did not find out about the three additional MFRs until (b) (6), (b) (7)(C) provided them to [redacted] after A1C Teixeira was taken into custody on 13 Apr 23. (Ex 43:174, 179) (b) (6), (b) (7)(C) had two different opportunities to provide the MFRs, but elected not to do so. Regarding the MFRs, (b) (6), (b) (7)(C) stated:

> Looking at the dates of those MFRs that [(b) (6), (b) (7)(C) handed to (b) (6), (b) (7)(C), if [redacted] or anyone had come up to us and said we think this is something, I would have immediately called OSI. I would've had my fact-finders come and meet with us--they have no problem coming down here in sitting with us--and bringing everyone into a huddle. But, no one ever did. (Ex 43:174-175)

After (b) (6), (b) (7)(C) discussion with the SSO, (b) (6), (b) (7)(C) did not discuss A1C Teixeira with anyone else. (b) (6), (b) (7)(C) never followed up with (b) (6), (b) (7)(C) (Ex 36:89) (b) (6), (b) (7)(C) did not raise any concerns with (b) (6), (b) (7)(C). (Ex 34:15)

(b) (6), (b) (7)(C) said (b) (6), (b) (7)(C) told [redacted] at some point after [redacted] sent [redacted] the MFRs that everything with A1C Teixeira "was good." (Ex 44:81) (b) (6), (b) (7)(C) testified, "it was a very brief conversation of, 'Hey, just so you know, I talked to [A1C Teixeira]. We're good,' like…kind of in the sense of, like, nothing to worry about, like, 'I've taken care of it. I've handled it as the [redacted] type." (Ex 44:81)

(b) (6), (b) (7)(C), was made aware of three of the four incidents concerning A1C Teixeira but delivered a substantially minimized version of the concerns to the SSO, adding [redacted] opinion that A1C Teixeira was simply curious and had an honest interest in cross training to the intelligence career field, which was not true. (Ex 40:33) [redacted] never provided the three MFRs, all dealing with seriously questionable security behaviors, to the SSO. As a former SSO [redacted], (b) (6), (b) (7)(C) should have been more forthcoming with the information [redacted] had in [redacted] possession at the time. In this regard, (b) (6), (b) (7)(C) also failed to meet the reporting requirements directed by DoDM 5200.01 V3 and DoDM 5105.21 V1. (b) (6), (b) (7)(C) should have thoroughly informed the SSO and provided the documentation in his possession in accordance with both DoDM 5200.01 V3, *Information Security Program: Protection of Classified Information*, which states, "Actual or potential compromises involving SCI shall be reported to the activity SSO…"; and DoDM 5105.21 V1, *SCI Administrative Security Manual: Administration of Information and Information Systems Security*, which states each individual who has access to SCI shall "Immediately report an actual or potential security violation or compromise to an SCI security official (SSO/SSR)." (Ex 20:100; Ex 17:15) A1C Teixeira violated both these regulations, which should have prompted reporting. (b) (6), (b) (7)(C) confirmed (b) (6), (b) (7)(C) never informed [redacted] of these issues with A1C Teixeira. (Ex 34:15) (b) (6), (b) (7)(C) [redacted]

After interviewing the supervisory chain, including the squadron, group, and wing commanders, knowledge of these security incidents was not fully disclosed to leadership in the 102 ISRG above the (b) (6), (b) (7)(C) beyond notification to the (b) (6), (b) (7)(C) informed (b) (6), (b) (7)(C), on some, but not all the incidents, and (b) (6), (b) (7)(C) was given assurances from (b) (6), (b) (7)(C) that [redacted] would bring those issues to the SSO. During [redacted] interview, (b) (6), (b) (7)(C) provided documentation for 15 incidents since taking command to illustrate that whenever he was properly notified of issues, [redacted] has taken action in a timely manner. (Ex 36:37, 132; Ex 93) (b) (6), (b) (7)(C) stated when something happens, "within 24 hours I'm talking to the SSO." (Ex 36:132) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C), were not made aware of concerns with A1C Teixeira until after A1C Teixeira's arrest.

Culpability of Others with Some Knowledge of A1C Teixeira's Questionable Activities

Although there are three major actors that had the most knowledge, responsibility, and culpability in failing to report A1C Teixeira's activities, other unit members who witnessed his

actions and reported them only to their supervisors, likewise should have reported these same concerns to the SSO directly. The "Know Your Why" culture likely contributed to this. While it is somewhat understandable a junior member, having reported concerns to their supervisor or squadron leadership, could be assured the matter would be properly reported to the SSO, the facts do not bear that out. While the knowledge of (b) (6), (b) (7)(C) , and others is less extensive than that of (b) (6), (b) (7)(C) , all unit members nevertheless had a responsibility to report matters to the SSO, and yet failed to do so.[32]

Indirect Contributing Factors

Inconsistent Reporting Guidance

DoD and AF guidance clearly states actual and potential compromises involving SCI must be reported to the SSO. 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. 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 the ISSO first, and not necessarily the SSO, as required in this case.

When discussing "security concerns" there are several diverse areas and facets related to the protection of classified national security information (CNSI), and different areas may have different reporting requirements, different definitions, and different Offices of Primary Responsibility (OPR). Some of those security-related areas include; counterintelligence, cybersecurity, general security, industrial security, information security, insider threat monitoring, National Background Investigation Services, operations security, personnel security, physical security, and Special Access Programs (SAP).

Different classification levels (TS, SCI, Secret, CUI) have different reporting requirements (whether concerns are to be reported to the SSO, commanders/directors, security managers, supervisors, or some combination thereof), which causes confusion, uncertainty, and/or inconsistency in how things are reported. In addition, reporting requirements that switch from "and" to "or" to "and/or" could result in confusion and underreporting. For example:

> **Unauthorized Disclosure (SCI)**. For matters involving the reporting of unauthorized disclosure or compromise of sensitive compartmented information (SCI), individuals are

[32] DoDM 5105.21, V3, 14 Sep 20, Enclosure 5, para 2: "It is the responsibility of all SCI-indoctrinated personnel to report any security incidents affecting or involving SCI to the appropriate SSO or local SCI security official." (Ex 18:54)

instructed to report to the appropriate special security officer (SSO), local SCI security official, *or* special security representative (SSR). (DoDM 5105.21-V1, Enclosure 2, para 12.b & DoDM 5105.21-V3, Enclosure 5, para 2.a, "Security Violations" are defined in part as a "compromise of classified information to persons not authorized to receive it.") (emphasis added)

Security Incidents. For matters involving the reporting of security incidents involving classified information, individuals are instructed to report to their commander *or* director, supervisor, *and* security manager who then shall report the incident to the responsible information protection (IP) office. (DoDM5200.01V3_AFMAN16-1404V3, Encl 6, Para 3g) (emphasis added)

Security Incidents (SCI). For matters involving the actual or potential compromises involving SCI shall be reported to the activity SSO and handled in accordance with DoD Manual 5105.21, Vol 1, and Intelligence Community Directive (ICD) 701. (DoDM 5200.01 V3, Enclosure 6, para 5.d) (Additional reporting requirements exist for incidents which have or may have significant consequences and/or may contain information from another IC element.) (See also DoDM 5105.21-V3, Enclosure 5) (emphasis added)

Reportable Actions. For matters involving reportable actions by others to ensure the protection of classified information or other information, individuals are instructed to report to ("shall alert") commanders/directors, security managers (assistants), *or* supervisors. (DoDM 5200.02-AFMAN 16-1405, Enclosure 6, para 1) (emphasis added)

Reportable Actions (SCI). For matters involving any information that could reflect on an individual's trustworthiness or on that of other individuals who have access to SCI, members are instructed to report to the proper authorities (SSO, security official, supervisor). (DoDM 5105.21-V1, Enclosure 2, para 12a) (emphasis added)

Continuous Evaluation. Personnel having access to classified information will be aware of and comply with periodic reinvestigation (PR), continuous evaluation (CE), and reporting requirements and will report information to the immediate commander *and/or* servicing information protection office (IPO) that may impact an individual's security clearance. (DoDM 5200.02-AFMAN 16-1405, Section 11, para 11.2.c) (emphasis added)

Currently, there is an independent publication review being conducted at both DoD and DAF levels to look into many of the controlling guidance on reporting security incidents. While this investigation does not look to duplicate that effort, evidence indicates inconsistent reporting guidance decreases accurate and timely reporting. It is strongly recommended all DoD and DAF guidance be standardized with consistent reporting requirements to both leadership and security, with a requirement to crosscheck and report all notifications.

Conflation of System Access and "Need to Know" Principle

There were indications 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 tacit 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. Computer/IT specialists require system access in order to perform system maintenance, but do not require access to intelligence content or products in order to maintain the system.

Examination of the multitude of standards on the topic of the proper handling of Top Secret information and access to information by certain individuals invariably turns to the topic of the "need to know" requirement. In simplest terms, that is a requirement to make sure an individual, who has the proper security clearance, and properly executed agreements such as a non-disclosure agreement, also has the required need to know the information in question. Under this provision, someone could have a TS-SCI clearance, but may not have the requisite need to know the information. It is one of the hallmarks of a compartmented security classification system.

In most cases, the concept of need to know is presented in current guidance as a responsibility of the individual granting access to classified information. For example, Executive Order 12968, 2 Aug 95, which establishes the basis of classified handling, 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. (Ex 14:4)

DoD Manual 5105.21v3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities*, 19 Oct 20, IC 2, 14 Sep 20 provides a more comprehensive definition and tells us in relevant part:

> THE NEED TO KNOW PRINCIPLE. The primary security principle in safeguarding SCI is access only by those persons with an appropriate clearance, access approval, clearly identified need to know, and appropriate indoctrination. Even when approved for a specific access, the holder is expected to practice need to know in acquiring or disseminating information about the program(s) or project(s) involved. (Ex 18:11) (emphasis added)

102 IW/SSO emphasize the importance of need to know and to seek guidance during their initial and annual refresher training:

> When in doubt ask. It is a violation if you fail to do so and you will be held responsible. (Ex 122:9)
>
> Your accesses will allow you to work/visit the SCIF's [sic] on Otis unescorted. This does not validate your need to know to all projects, caveats, or computer systems. When in doubt…ask!!!!! (Ex 110:11; Ex 122:8) (emphasis added)

The approach that need to know was a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information was appropriate when most classified was transferred and maintained in a physical form. However, this approach becomes insufficient with the growing abundance of electronic classified information in a cyber landscape. While some standards addressing the need to know principle have been appropriately expanded, considerations for electronic dissemination are addressed in a limited number of security standards. This inconsistency should be addressed in the existing directives and instructions; specifically, policy should require verification of user authority before giving information, and an onus on the user to only access need to know information required for their duties. During the course of the investigation, in comparing the published guidance and requirements with current practices, it was apparent the lines between system access and need to know were blurred—especially with respect to a systems administrator's access. (Ex 43:103; Ex 48:74) Systems maintenance personnel may require access to resolve issues or repair networks but not for access to intelligence information or analysis.

(b) (6), (b) (7)(C) touched upon the concept of need to know during [redacted] testimony when [redacted] directed A1C Teixeira to "cease all research where he did not have a need to know." (Ex 50:2) Potentially complicating clear lines of distinction, as discussed earlier, encouraging a unit culture where all members of the 102 ISS were integrated into the overarching mission and having an interest in intelligence operations was encouraged. Explaining the "why" of each Airman's daily work was used to motivate Airmen. This led to including systems maintenance personnel in weekly TS-SCI intelligence briefings. (b) (6), (b) (7)(C) agreed with the concept but believed that "a line should have been drawn somewhere" between operations and support personnel. (Ex 87:2)

(b) (6), (b) (7)(C) likewise, acknowledged the concept of need to know, pointing out in [redacted] role, as the (b) (6), (b) (7)(C) even [redacted] did not have a need to know intelligence analysis information. (Ex 38:21)

When asked about need to know during [redacted] interview, the former (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) described the relationship between security clearance, system access, and need to know; and whether providing intelligence briefings to systems maintenance personnel could have caused confusion about whether IT specialists had a need to know other classified information. He maintained providing briefings did not cause confusion about need to know, although other witnesses interviewed held up the briefings as examples of how leadership

endorsed and encouraged curiosity on intelligence matters for non-intelligence members of the unit. (Ex 41:11; Ex 44:18; Ex 49:70) (b) (6), (b) (7)(C) explained, "A security clearance is the baseline to get in the building, the access is what they needed access to, in order to facilitate whatever mission functions, requirements that needed to occur." (Ex 39:23) He said need to know was "need to execute the mission." When asked whether IT specialists using their access to gain additional information outside of their assigned mission was need to know, (b) (6), (b) (7)(C) responded, "Yeah, that's not the need to know. That's outside the bounds of where their need to know lies." He further clarified he did not give IT specialists the know-how to explore classified systems. (Ex 39:23-27)

(b) (6), (b) (7)(C), was asked about need to know and confirmed (b) (6), (b) (7)(C) understanding that JWICS access was afforded to 1D systems maintenance personnel only to facilitate performing their IT duties, but that access did not mean they had permission to freely explore information on JWICS. (Ex: 184-185)

Similarly, (b) (6), (b) (7)(C) was asked to comment on how the Services apply need to know in daily operations. [redacted] was asked to comment on the concept of system access versus need to know, specifically, if system access for systems maintenance people and JWICS access created or justified a need to know for intelligence information. [redacted] responded:

> [redacted]: No, it does not. The problem is that--I don't know if you're going to ask questions about the mechanisms that we use to validate need to know, but I think that's broken.
>
> IO: Please…share that. What your thoughts are on that?
>
> …
>
> [redacted]: Joint Entitlement Management System. It's the mechanism that they put in place after Snowden to--so the way the system works, in a nutshell, is once you get access to JWICS, you just got a login, right? You can apply to get a PKI certificate. Unlike… NIPR and SIPR, where you have a physical token, the PKI certificates are purely digital. So, you go through this process. Each site has a trusted agent. [redacted], I think, is a trusted agent here. And 16th Air Force creates this certificate for all the Air Force JWICS users. And then that is, no kidding, you use that digital certificate. It identifies you as a persona. So that when you go to websites, there's a handshake behind the scenes that says, "Hey, this is who I am." And then there's this thing called JEMS, the Joint Entitlement Management System, that says, okay, well this is what this person has a valid need to know for. When you first get that certificate, you go into JEMS and you say--there's different boxes you can check, that you can select. For example, you need to know things about a specific AOR, a specific type of weapon system, surface-to-air missiles, aircraft, what-have-you, or different types of intelligence. So like HUMINT, IMINT--imagery intelligence, signals intelligence. So you can check those boxes, then you--it's got a justification block. You type in what you're justify–why you need access to those things, and then you hit submit. It goes off and it gets validated by someone. The last time I…did it has been–it's been a

> couple years, so I don't know what it is today. But back then, when I had to submit my need to know, you go through and you sit and it asks you what organization you're a part of. So you go, Air Force, 16th Air Force, 480th ISR Wing, because that's who we work for. And then it goes to some validator at–at the 480th–or it did back then–who is determining the need to know for everyone across the Air Force DCGS enterprise. What is it, 7,000 Airmen? So I don't know how big that shop is, but that's a lot to ask. So, I was interested when the SECAF memo came out because it has in there – I think that it's a commander's responsibility to determine need to know. Well, that'd be great if we had a local validator. But I don't have a local validator, you know, so I hear, if you had a trusted agent who was local making that need to know determination, it could have been whoever. So maybe down in the weapons and tactics shop, one of the NCOs down there would have said, "Why does a 1D need access to – to this stuff?" I think JEMS is a–was a great idea. It was–I don't know if it was implemented the right way. Obviously, this [has] shown that. (Ex 35:118-120)

A more complete discussion of the Joint Entitlement Management System (JEMS) system is covered in the classified supplement to this report.

Likewise, [redacted] was asked [redacted] thoughts on the balance between access and need to know. [redacted] explained, "I think the way we do ISR operations today, don't fit that really neat 'need to know' where we're…you know, we're not in little compartments, we're not in little rooms…I don't know how in an open storage facility that's--that you have those caveats and read-ins, that information is there. It's up on giant screens." (Ex 33:82) [redacted] explained that computer/IT specialists, such as A1C Teixeira, were given access to JWICS to execute their duties. But their access to JWICS also gave them access to Top Secret information for which they did not have a need to know. (Ex 33:83-85)

Post-9/11 concerns regarding insufficient intelligence sharing have moved decisively in the direction of increased access without providing appropriate controls or monitoring for need to know. If there is a requirement to allow expanded access in the interest of intelligence sharing, that access must come with enhanced visibility to detect concerns or have a more robust and timely access approval system.

Differences in Disciplinary Action Between T32 and T10 Members

To support its federal (T10) mission, numerous 102 IW members are placed on T10 orders. Due to their federal status on T10 orders, ADCON for these members, including discipline, falls to the 201 MSS at JB Andrews. T32 commanders could complete disciplinary actions on T32 Airmen locally using the Massachusetts Code of Military Justice (MCMJ). (Ex 37:70) However, per DAFI 51-201, *Administration of Military Justice,*[33] DAFI 51-202,

[33] DAFI 51-201, *Administration of Military Justice,* para 3.6.2.2, "prior to taking judicial action against an ANG member, legal offices, commanders, and convening authorities at all attached Regular DAF unit or host commands must coordinate with 201 MSS through ANGRC (NGB)"

Nonjudicial Punishment,[34] and 201 MSS policy, disciplinary actions for T10 personnel had to be coordinated with the 201 MSS/CC prior to taking action. (Ex 136, Ex 137, 117) A visual depiction of the T32 and T10 ADCON lines of authority are depicted here:

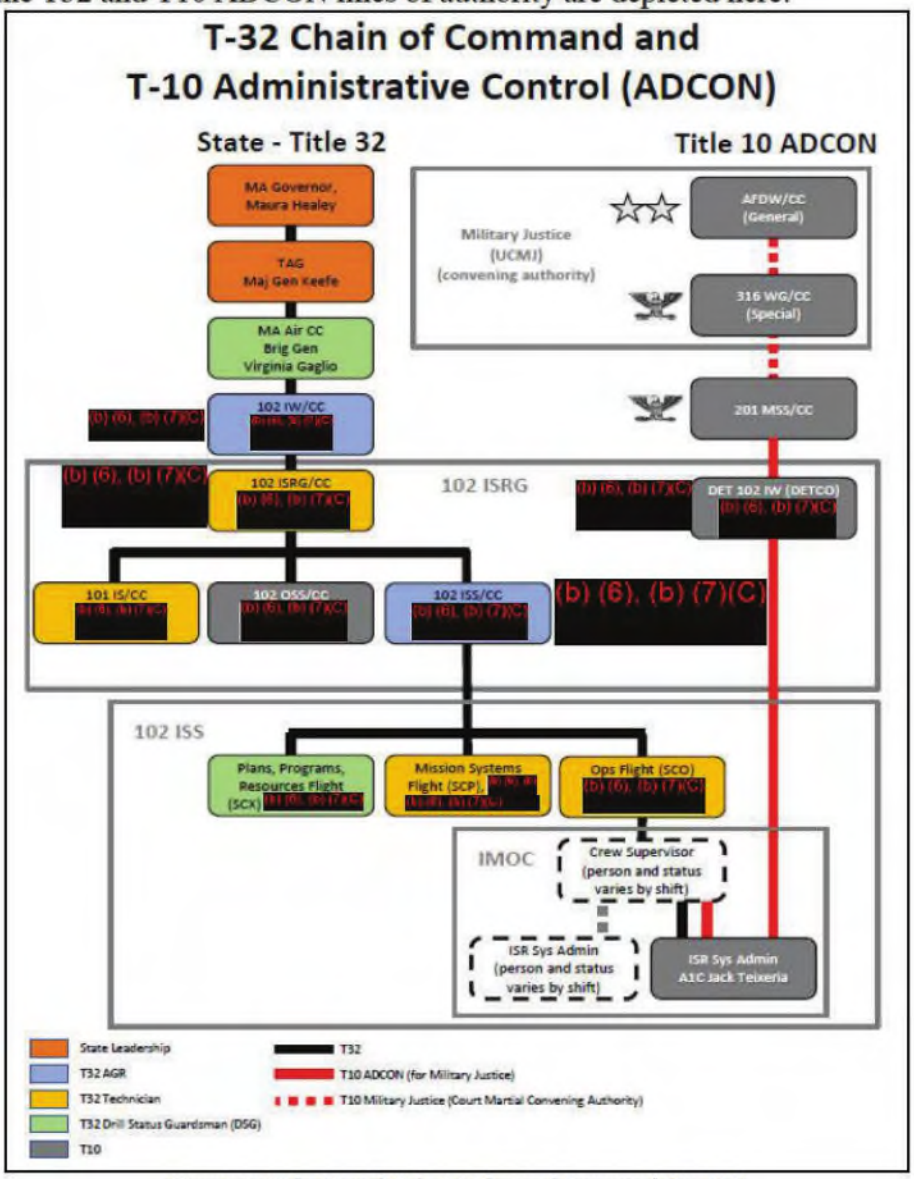

Figure 5: Title 10 and Title 32 Chain of Command (Ex 114)

[34] DAFI 51-202, *Nonjudidicial Punishment,* para 1.2.1.3, "Coordinate with the administrative control (ADCON) commander to whom the Air National Guard (ANG) member is assigned when in Title 10 status or the 201st Mission Support Squadron (MSS) commander prior to initiating NJP action against an ANG member assigned or attached to the commander's unit, whichever is applicable.)

According to some witnesses, this coordination with the 201 MSS T10 chain could take additional time to accomplish disciplinary actions. (Ex 33:14; Ex 37:46) (b) (6), (b) (7)(C) According to (b) (6), (b) (7)(C) is responsible for disciplinary actions and administrative corrective counseling of 5,000 to 10,000 T10 Airmen. (Ex 34:3) also testified that in 2022, was responsible for overseeing 20,000 members on T10 orders worldwide at any given time. (Ex 34:4)

(b) (6), (b) (7)(C) following the UD, was asked about this dynamic for taking administrative action among T32 members versus T10 personnel. responded, "Oh, as a commander, I'm frustrated." (Ex 37:46) continued:

> [I]f I can't enact corrective action in a timely manner, it starts to lose its meaning. And it's frustrating when I have another entity that I can't do anything about and it's jammed up. And I feel like it—it frustrates me for a couple different reasons. And if it's in an instance where there's a, I'll use the term "victim," but if there's somebody else out there that's looking for a wrongdoing to be corrected and it's jammed up because of a bureaucratic process, I look like I failed that Airman and that Airman starts to lose confidence in us as a unit and us as leaders and that's—that drives me crazy.
>
> …
>
> So I feel like it's a lot more expeditious on the Title 32 side, but to an Airman, they don't really care what status they're in, they just kind of want to see that things are being done. And—you know—not all Airmen are bad, I just want to be able to give corrective action so they can learn and move on. (Ex 37:46)

(b) (6), (b) (7)(C) was also asked if was prohibited from taking swift action because of the requirement to send administrative actions up through the T10 chain of command first. explained it was frustrating to that there was a delay in processing the paperwork, but would nevertheless not wait to take action or intervene to correct behavior on the spot. (Ex 37:47) In support of this offered an example:

> [C]ase in point right now. It was an Airman where I decided to pull his clearance. Technically, he doesn't belong to me because he's Title 10, but I did the action and reminded him, like, "Look, you technically belong to (b) (6), (b) (7)(C) the 201st Mission Support Squadron Commander, but I'm doing this action now because the behavior is the behavior, and we'll worry about the formality of your LOR when it gets to that point." And then when I read him his LOR, I said, "As a reminder, my name is not on this, it's

(b) (6), (b) (7)(C), but it doesn't change the fact of what I did to you 2 weeks ago, it just took me a while to get the administrative action done." (Ex 37:48)[35]

(b) (6), (b) (7)(C) testimony added validity to the concerns when it comes to processing administrative actions for T32 and T10 Airmen.

For [redacted] part on this topic, (b) (6), (b) (7)(C) commented that the time delays for T10 Airmen were more impactful and detracted from unit effectiveness. (b) (6), (b) (7)(C) was asked about [redacted] thoughts on the 201 MSS role in T10 discipline:

> IO: [W]hat are your thoughts on that? Do you, do you have any…concerns that there's a segment of the population…that's yours on this installation, but in a way, they're not; that if there's…issues with them, then you have to work that up the Title 10 chain. That is, you know, having the stick on one hand, but not the hammer to go with it. What are your thoughts on that?
>
> [redacted]: I guess I'll say my thoughts on it aren't relevant.
>
> IO: What do you mean it's not relevant?
>
> [redacted]: I—[chuckled]. Well, I guess, what I—I don't know. I guess my thoughts—I mean, they've made a—they've made a command decision on how they're going to do—to do this. Right?
>
> IO: Sure.
>
> [redacted]: Um, and we've saluted smartly and we're—we're going to go—we're going to go through it, you know
>
> …
>
> [A]nd see how it goes.
>
> IO: Okay. Well, I mean, we typically salute smartly and press on when—ideally, in a perfect world, you know, king for a day, if you could change that, if you—if you did have that authority—and by the way, you know, part of our charter here…is to come and see Air Force wide, DoD wide, other issues that we could make some changes on, that would help, help someone that's…in your seat. (Ex 33:12-13)

Referring to the 201 MSS, (b) (6), (b) (7)(C) responded:

---

[35] (b) (6), (b) (7)(C) was assessed as a highly credible witness. [redacted] judgment and leadership appeared to set the bar in the 102 ISRG. The majority of witnesses interviewed in-person at the 102 ISRG requested (b) (6), (b) (7)(C) for their warm handoff at the conclusion of their interviews.

> So, having been here a long time, having, you know, dealt in this mission since 2008, having been the Title 10 Detachment Commander…the amount of "Choke-Con"[36] that they want, ebbs and flows by who the 201st MSS Commander is. (Ex 33:13)

[redacted] voiced the opinion that from a policy perspective, administrative actions should be handled at the base, by the T32 chain of command, while the T10 chain should be involved in higher level actions such as Non-Judicial Punishment (NJP):

> [P]reviously, we had the ability to certainly give an Airman a Letter of Counseling and deal with that, um—and then I really, ah, think that, that's the way it should be and if the misconduct is so egregious that we're going to have to go with NJP and under the UCMJ, then that will be the time to involve them [201 MSS].
>
> [T]he other issue is, um, if you're dealing in the Title 10 world, the servicing JA office is Hanscom Air Force Base, and I'm sure they have a lot of their own business and I'm sure that any of my business seems to go to the end of—of their pile. Like…for example, we will have a Letter of Counseling sit up for legal review for four months. (Ex 33:13-14)

In summary, [redacted] opined, administrative actions for T10 Airmen at Otis ANGB would be better served by the local chain of command. In describing the nuance to Airmen, of the difference, he explained:

> [I]t's equitable. It's quicker. And…you know, it's done at the appropriate level. I mean, our Airmen don't know who [redacted] or…you know, [redacted] are or how that works, right? Regardless of the status they're in, we're the face of the—the agency, the unit, and…those are our Airmen. (Ex 33:19-20)

It is noteworthy that [redacted] was aware of the timeliness issue regarding disciplinary actions on T10 members versus T32 members but did not address those concerns with [redacted] (Ex 34:24)

A review of 201 MSS administrative actions applied to the 102 IW as well as other, similarly situated Wings, shows instances where it took greater than 30 days to process and approve administrative actions. (Ex 124) While [redacted] testified it was not [redacted] intent to require permission prior to taking action, it was required by [redacted] published guidance. For example, the 4 Nov 21 NGB memo makes it clear ANG members on T10 status are assigned to the 201 MSS for ADCON, and commanders with T10 members are:

> required to communicate planned command action regarding any of the following before initiation (or as soon as possible after doing so) if circumstances require: Record of

[36] Informal term meaning the OPCON/ADCON difference creates a choke point or bureaucratic/administrative delay.

> Individual Counseling (RIC), Letter of Counseling (LOC), Letter of Admonishment (LOA), Letter of Reprimand (LOR). (Ex 117) (emphasis added)

As touched upon here, some commanders and SNCOs at Otis ANGB felt this disparity between T32 and T10 Airmen 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 MFRs instead of RICs, LOCs, LOAs, or LORs. The approach of overusing 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. The other issue with MFRs is they were not, by design, routinely provided to Airman or the SSO. In some cases, documentation was collected on Airmen without their awareness. (b) (6), (b) (7)(C) on Regularly Scheduled Drill (RSD) periods, testified:

> I think, at least to me, an MFR is just a record of a conversation. So I don't think it's normal practice across--like, the [101] IS as well, like, I have 10s of MFRs on people being tardy, but I never give it to them. We've had a conversation; they know it happened, I know it happened. I'm just documenting it for my record.
>
> IO: At the [end] of that conversation, is it common to say, like, "I'm going to document this in an MFR and it will be added to your…folder," or no?
>
> (b) (6), (b) (7)(C): I would say that's not a common practice here to say that. (Ex 44:46-47)

Since local commanders and SNCOs expressed concern with having to wait to administer progressive discipline until well after the incident in question, this lack of immediacy could further affect good order and discipline. This, in turn, may have diminished the likelihood and severity of the administrative actions and reduced the opportunities for such conduct to be reported to the SSO, thereby impacting overall security.

While at Otis ANGB, IG investigators found supervisors had a tendency to utilize MFRs to document corrective action, since their perception was that MFRs were easier or quicker than going through the 201 MSS coordination process. (b) (6), (b) (7)(C) commented on this:

> So I would say that perception probably is something that they [102 IW] carry along, maybe historically there. But again, the barrier to entry--I mean, the irony here is if they have a [Title 10] DETCO,[37] the barrier to entry is--the DETCO is right there, and so you would think it would numerically increase the number of data they were reporting.
>
> …

[37] (b) (6), (b) (7)(C).

> So I don't know. I don't mean to be harsh. That just seems like a bit of a cop out of maybe people who are pointing fingers [on] the Title 32 side…of not notifying or not talking. And certainly--and additionally, as an intel person, the barrier to entry to report, for SSO and Insider Threat Hub, are even frankly more of a universal obligation. So that stuff should have been done regardless…. (Ex 34:26)[38]

(b) (6), (b) (7)(C) did not believe this view was widespread elsewhere, and believed that was "something that is culturally unique then to Otis."[39] (Ex 34:24) [redacted] added that if this was a concern from the 102 IW, it had not been brought to [redacted] attention:

> And that probably doesn't have a ton to do with the 201st. So–for a few reasons. If the speed or the rapidity of the actions were problematic, given how much we talked to (b) (6), (b) (7)(C), I think I would have taken some of that feedback directly. (Ex 34:24)

(b) (6), (b) (7)(C) was asked if [redacted] thought there could be some allowance for lower-level administrative actions to be issued at the base level, if the unit kept the 201 MSS informed, but [redacted] did not favor this approach. [redacted] was asked if it would be alright if an LOC, a fairly low-level administrative action, could be issued without [redacted] seeing it first.

> I would definitely want to look at what they did, right? It would depend on what they did it for. So for example, like, let's say that someone counseled Airman Teixeira for doing something kind of related to this. Like, they caught him browsing or they caught him printing or something. If they inform me about an LOC for that, I would stop the process and discern like, "Okay, did you talk to the SSO? Did you talk to…"--there are some things where you want to--basically they--you would stop and drive down another path. (Ex 34:25)

(b) (6), (b) (7)(C) and previous 201 MSS/CCs issued policy memos and guidance to DETCOs, on the topic of coordinated disciplinary efforts. The guidance, which had to be signed and returned by the DETCOs makes it clear, in relevant part:

> The 201st Mission Support Squadron Commander (201 MSS/CC), Joint Base Andrews, MD, exercises ADCON over all Air National Guard (ANG) members who become a part of the Air National Guard of the United States (ANGUS) in Title 10 (T10) status. This authority can be delegated to assigned Detachment Commanders (DETCOs) acting in coordination with, and on behalf of, the 201 MSS/CC as the ADCON Commander. Appointed DETCOs act as a direct link between their T10 members at the unit level and

[38] A discussion of the capabilities of the DAF C-InT Hub is discussed in the classified addendum to this report.
[39] The DETCOs of other similarly situated units were also interviewed, namely 119 WG, 181 IW, and 184 IW. In summary, these units acknowledged some of the difficulty involved with coordinating all actions with the 201 MSS. Some of the units took a more hands-on and proactive approach to discipline, while trying to stay within the policy guidance more generally. (Ex 55:2; Ex 57:2)

the 201 MSS/CC; they also exercise delegated ADCON authority on behalf of the 201 MSS/CC.

…

The DETCO's ADCON command authority is derived from, and subordinate to, the 201 MSS/CC.

- DETCOs must inform the 201 MSS/CC of T10 DET ADCON issues.

- When a member of your T10 DET is involved in a matter where disciplinary action is contemplated or being considered, you must coordinate with the 201 MSS/CC prior to taking action. If the 201 MSS/CC concurs with the proposed action, you may be instructed to carry it out on his/her behalf. At no time should you carry out disciplinary action without this coordination.

- The DETCO will report monthly to the 201 MSS/CC on the status of T10 DET ADCON issues. (Ex 118:1) (emphasis added)

Overall, it is worth noting the 201 MSS has a small staff. They are responsible for thousands of administrative and disciplinary actions for T10 Airmen across the globe. All disciplinary actions for T10 personnel must be coordinated with the 201 MSS/CC prior to taking action. As a result, it can sometimes take months to accomplish a low-level administrative action, such as an LOC. This structure gives reach back authority for deployed Guard members.

The shift, by some ANG units into "employed in place" missions such as cyber and intelligence, has overwhelmed the system and structure in place with a heavy workload. Whether intended or not, there is validity to the concerns about timeliness and efficiency when processing administrative action for T32 and T10 Airmen. There are valid reasons to consider adjustments to the ADCON chain of command. Commanders reported they were frustrated having to wait to take action for T10 personnel, compared to being able to take prompt action to correct T32 personnel, and stated the time delays for T10 Airmen were more impactful than for T32 Airmen and as such, detracted from unit effectiveness.

The [redacted] voiced the opinion that from [redacted] perspective, administrative actions should be handled at the base, by the T32 chain of command, while the T10 chain should be involved in higher level actions such as NJP. [redacted] felt such an adjustment would be quicker, more equitable, and handled at the appropriate level. A review of 201 MSS administrative actions applied to the 102 IW as well as other, similarly situated Wings, confirmed instances where it took greater than 30 days to process and approve some of these administrative actions. (Ex 124) Frontline supervisors might tend to avoid coordinating with the 201 MSS entirely by simply opting to give verbal counselings or writing MFRs instead of RICs, LOCs, LOAs, or LORs. Other similarly situated units related that on occasion they exercised their own judgment and advised 201 MSS after the fact. There was evidence that MFRs were over-utilized at the

expense of progressive discipline, and in turn, notification and tracking by the SSO. (Ex 35:67; Ex 44:46) [redacted] testified [redacted] had never been given feedback about these concerns from leadership at Otis ANGB. However, given that most administrative discipline letters include the date of the misconduct, the timeliness issues should have been readily apparent to [redacted] and [redacted] staff. Collectively, while not directly causal to the unauthorized disclosures, it would be worth revisiting this T10 ADCON structure in the interest of either providing additional resources to manage the number of Airmen on T10 orders at any given time, or consider policy or legislative changes to allow the T32 chain of command to take lower level administrative action on their Airmen in T10 status.

Lack of Supervision/Oversight of Night Shift Operations

Witness testimony indicated there was a lack of supervision during night shifts in the 102 ISRG. [redacted] According to [redacted] when there were no intelligence missions at night, members of his 3-person crew were the only personnel in the SCIF. (Ex 65:1) Their primary role was to ensure the Heating, Ventilation, and Air Conditioning (HVAC) system was operating properly and answer the phones. (Ex 65:1) While on shift, their manning requirements were:

- One person had to be in the building, preferably near the IMOC desk to answer phone calls and respond to HVAC alarms
- Second person had to be able to respond within 5 minutes
- Third person was a floater--allowed to go to the gym (Ex 65:1)

Sometimes members were required to perform Preventive Maintenance Inspections (PMI) and other tasks throughout the SCIF, which required individuals to be on their own for hours, unsupervised in other parts of the SCIF. (Ex 65:1)

[redacted] was the third person on [redacted] crew, working with A1C Teixeira. (Ex 72:1) [redacted] stated their crew had a lot of free time after completing their assigned tasks, and could go to the gym for an hour. (Ex 72:1) [redacted] also stated [redacted] took a lot of leave (about 1 day/week), leaving just [redacted] and A1C Teixeira on shift those nights.

In summary, 102 ISS personnel were required to work 24/7 in the open-storage SCIF, even when no operational missions were taking place, to monitor the building's HVAC system. (Ex 65:1) During these periods, only 2-3 personnel were present in the SCIF, and they had access to a master key for every office in the two-story facility. (Ex 48:29) Further, no permission controls were in place to monitor print jobs, and there were no business rules for print

products. (Ex 48:37; Ex 49:32) Any night shift member had ample opportunity to access JWICS sites and print a high volume of products without supervision or detection. 102 ISS shift manning, unsupervised work, and the physical layout of the SCIF would have provided A1C Teixeira the opportunity to print intelligence products and physically remove them on a regular basis without being discovered. A more detailed analysis of A1C Teixeira's online access and activities is provided in the Classified Annex to this report. (Ex 125)

Results of Defense Counterintelligence and Security Agency (DCSA) Field Investigations for Security Clearances Not Provided to Units

For new enlistees, a recruiter works with the prospective member and the wing Information Protection Office (IPO) to prepare a properly completed Standard Form 86 (SF-86) *Questionnaire for National Security Positions*, typically utilizing the electronic application (eApp), which is replacing the Electronic Questionnaires for Investigations Processing (e-QIP). The wing and MAJCOM IPOs review the eApp for accuracy and completeness and forward it to the DCSA for processing. A DCSA investigator conducts field interviews and collects data which is forwarded to the Consolidated Adjudication Services (CAS) (formerly Consolidated Adjudication Facility or CAF) for adjudication.

The CAS adjudicator reviews collected data based on a "whole-person" concept, according to federal guidelines in 13 categories: Allegiance to the United States, foreign influence, foreign preference, sexual behavior; personal conduct; financial considerations; alcohol consumption; drug involvement and substance misuse; psychological conditions, criminal conduct, handling protected information, outside activities, and use of information technology. (Ex 16:6)

If the member's prior conduct raises concerns, the adjudicator is instructed to judge the overall relevance of the conduct by considering: the nature, extent, and seriousness of the conduct; the circumstances surrounding the conduct, to include knowledgeable participation; the frequency and recency of the conduct; the individual's age and maturity at the time of the conduct; the extent to which participation is voluntary; the presence or absence of rehabilitation and other permanent behavioral changes; the motivation for the conduct; the potential for pressure, coercion, exploitation, or duress; and the likelihood of continuation or recurrence. (Ex 16:6)

Additionally, when information of a security concern is known, the adjudicator should consider whether the individual voluntarily reported the information, was truthful and complete in responding to questions, sought assistance and followed professional guidance where appropriate, resolved or appears likely to favorably resolve the security concern, and has demonstrated positive changes in behavior. (Ex 16:7)

On initial clearances, adjudicators typically make a binary Favorable or Unfavorable determination on the security clearance and the wing is notified via the Defense Information System for Security (DISS). Adjudicators can also make a Favorable determination with Conditions, but this is rare, and limited to situations where the information of concern can only be mitigated with additional security measures or monitoring. For example, a member with a bankruptcy may have to submit monthly financial statements to their Commander. (Ex 16:27; Ex 79:2)

A1C Teixeira signed his e-QIP on 18 Nov 19, (b) (6), (b) (7)(C) a senior in high school, then scheduled to graduate (b) (6), (b) (7)(C) (Ex 83:47) His background investigation was closed on 4 May 2020. (Ex 83:2) During his first security clearance interview, he disclosed he was (b) (6), (b) (7)(C), as his only job, but forgot to list it as employment. He denied having any issues at work and did not believe there was any record or testimony that would contradict his claims. (Ex 83:54) In reality, he was given formal written warnings from his employer, which he signed, on two occasions, once for missing a shift and another for having his cash drawer short by $16.11. (Ex 83:55-56) A1C Teixeira did not disclose or acknowledge these events until his third security clearance interview. A1C Teixeira told security investigators he did not provide this information during his first and second interview, when prompted, because he claimed he forgot about them or thought they were irrelevant. (Ex 83:56)

During his initial interview, A1C Teixeira did disclose he had difficulty getting a FID card because he was suspended from high school due to concerns he was going to commit acts of violence against the school. (Ex 83:53) At the time of the incident, the school [redacted] notified the local police department, which conducted an investigation. The police talked with [redacted] students who confirmed, while at a school assembly, A1C Teixeira told them he had a "molotov cocktail " in his bag and asked what they would do if he threw it. (Ex 83:68) A1C Teixeira claimed the molotov cocktail comments were taken out of context because they were talking about a World War II video game, Call of Duty; however, the two students noted the molotov cocktail comment was made prior to the video game discussion. (Ex 83:68) [redacted] students claimed A1C Teixeira made racist statements, saying he wanted to "kill all black people, black people don't exist, and I hate n*****s." (Ex 83:68-69) Several students reported he talked about killing squirrels and being violent with animals, and he was a gun and military history enthusiast. (Ex 83:68-69) [redacted] teachers stated A1C Teixeira was a "concern" per ALICE training standards.[40] (Ex 83:68) However, neither the students nor the teachers interviewed by the police department felt A1C Teixeira was a threat. As a result the case was closed with no further action. (Ex 83:69)

[40] According to the website www.alicetraining.com, begun in 2000, ALICE Training® (Alert, Lockdown, Inform, Counter, Evacuate) is a widely adopted, effective method of active shooter response training for workplaces, schools, and individuals.

Ultimately, A1C Teixeira was recommended for a position of trust by [redacted] (Ex 83:59, 63, 64, 71, 72) Despite the aforementioned negative information, the adjudication service, utilizing the "whole person" concept and federal guidelines described above, granted a favorable determination for a TS-SCI clearance and notified the 102 IW/IPO through DISS. As is standard practice, the IPO does not receive any of the additional background or field investigation information used by the adjudicators to approve members; they receive the clearance approval or disapproval and the effective date. (Ex 79:2) 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

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. The full report is at Exhibit 104.

Protection of SCI Material and Information Security (INFOSEC) Programs

The 102 IW INFOSEC program was not effective and lacked meaningful activity prior to 2023. The 102 ISRG SCI program lacked clear delineation of responsibilities between the SSO, Chief of Information Protection (IP), and Security Managers. 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. Examples of other non-compliance areas include local security instructions not meeting minimum requirements, improper maintenance of classified storage containers, lack of Emergency Action Plans, failure to enforce training standards, and improper marking of TS-SCI working papers. (Ex 104:4)

The AFIA inspection revealed a lack of INFOSEC inspection emphasis by 102 IW leadership. Compounding the problem, the Air Combat Command Inspector General (ACC/IG) did not identify any information indicating security concerns during an Oct 21 Unit Effectiveness Inspection (UEI).

The AFIA inspection discovered several missed opportunities for the 102 IW to address INFOSEC issues. In Oct 21, ACC/IG did not identify INFOSEC concerns during the 102 IW UEI. However, in Feb 23, the 102 IW/IG assessed a deficiency against the 102 IW/IPO for having no record or documentation of INFOSEC annual self-assessments, the conduct of Self-Assessment Checklists, and other mandated inspection program activities, which would have been evident during the period covered by the 2021 UEI. Later in 2021, a security incident occurred where a pallet containing classified materials and equipment was improperly shipped to Robins AFB, GA. (b) (6), (b) (7)(C) 102 IW/CC, initiated a Commander Directed Investigation (CDI) in Feb 22 to determine the facts and circumstances regarding this event. The materials and equipment were eventually discovered and properly sanitized and destroyed at Robins AFB. (Ex 128)

The findings of the CDI and the associated remedial actions focused on the specific circumstances of the incident. It was evident leadership viewed the security incident as an isolated incident. Further actions were not taken to identify or address the underlying causes of complacency, miscommunication, or lack of classified equipment accountability, or to address broader concerns with the INFOSEC program. The report also showed a lack of oversight and external communication between the 102 ISS and offices at various levels responsible for safeguarding classified information. The recommendations provided in the CDI focused on addressing the specific incident through improvement of shipment procedures and storage labeling, but also evidenced broader INFOSEC process concerns that were not identified and addressed, posing a higher risk to the protection of classified information within the unit. (Ex 128)

It was not until Feb 23 that INFOSEC was identified as a significant deficiency by 102 IW/IG. The failure to identify and correct deficiencies before this demonstrated a general lack of leadership emphasis, at all levels, on the importance of compliance with information security policies. (Ex 104:4)

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 102 ISRG members had not completed IO training. Supervisors did not facilitate the reporting of known and possible IO-associated violations or irregularities to the 102 IW/IG, 102 IW/SJA, or unit-level IO monitors. Finally, the unit's inconsistent enforcement of compliance with IO was concerning. (Ex 104:6)

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 commanders did not apply or enforce wing or group level direction. Interviews with 102 ISRG personnel indicated a lack of awareness and understanding of the program at all levels. Group and squadron program managers indicated that, apart from being trained, little-to-no direction or attention was placed on tracking compliance, correcting errors, or communicating risk. A more rigorous self-assessment program may have identified the INFOSEC and IO issues that contributed to this unauthorized disclosure. (Ex 104:7)

Unit Security Climate

Finally, 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. (Ex 104:13-17)

Additional Considerations

DAF Counter-Insider Threat Hub (DAF C-InT Hub)

The DAF C-InT Hub derives its authorities from Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," 21 Nov 12, and Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," 7 Oct 11, which together established the structure and minimum standards for an effective insider threat program across the Executive Branch. These criteria are further detailed by the Committee on National Security Systems Directive (CNSSD) No. 504, "Directive on Protecting National Security Systems from Insider Threat," September 2021, which lays out the requirement for User Activity Monitoring (UAM) and the ability to receive and coordinate insider threat related information from multiple offices. (Ex 73:1)

The DAF C-InT Hub receives its direction from DoDD 5205.16, *The DoD Insider Threat Program*, 30 Sep 14, Change 2, 28 Aug 17, and AFI 16-1402, *Counter-Insider Threat Program*

Management, 17 Jun 20. Specifically, it is tasked to collect, integrate, and analyze indicators of potential insider threats from multiple sources, to include; UAM, enterprise audit management, cybersecurity, law enforcement, counterintelligence, personnel security, human resources, command reporting, and medical and legal communities. (Ex 27:10) The AFI also establishes the designated Insider Threat Liaisons at the MAJCOM level to serve as the DAF C-InT Hub's link to units in the field. (Ex 27:8-9) Additionally, wing and installation commanders are directed to ensure any insider threat information from their command is reported to the MAJCOM-level Insider Threat Liaison. (Ex 27:10)

When properly executed, an Airman reports an insider threat concern to the wing IPO, who forwards it to the MAJCOM IPO/Insider Threat Liaison, who then files a report with the DAF C-InT Hub. The DAF C-InT Hub then conducts manual searches and queries on the various information systems within its jurisdiction and authorities to build a comprehensive threat picture. The results are typically offered first to AFOSI for possible criminal or counterintelligence investigation and are also shared with the "risk owners" and "information owners," with usually more than one agency involved. (Ex 73:1-2) The DAF C-InT Hub also analyzes the results for reporting thresholds in 13 different categories as established by the DoD Insider Threat Management and Analysis Center (DITMAC): serious threat, allegiance to the United States, espionage/foreign considerations, personal conduct, behavioral considerations, criminal conduct, unauthorized disclosure, unexplained personnel disappearance, handling protected information, misuse of information technology, terrorism, criminal affiliations, and adverse clearance action. (Ex 105:9) Typically, the DAF C-InT Hub handles approximately 2,000 cases per year. (Ex 73:2)

Additionally, the DAF C-InT Hub uses its UAM capabilities to track and record online and system activities and issue alerts based on a set of pre-defined criteria. These capabilities are discussed further in the Classified Annex to this report. (Ex 125)

As noted earlier, A1C Teixeira's supervisory chain failed to notify the SSO, IPO, and relevant authorities about his activities, which would have leveraged the full capabilities of the DAF C-InT Hub. However, a retroactive analysis of his recorded UAM activities revealed that while he had both a regular JWICS user account and an elevated "privileged user" account to accomplish his system administrator duties, all of his web and printing activity was accomplished through his regular user account. (Ex 82:1) It should be noted that his "privileged user" account, while not used, did not grant him access to additional JWICS sites, but rather allowed him to access and modify "behind the scenes" files required for his job (e.g., root files, user profiles, permissions, etc.). (Ex 78:1) A more detailed analysis of A1C Teixeira's online activities and recommendations regarding UAM are provided in the Classified Annex to this report. (Ex 125)

V. 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. (b) (6), (b) (7)(C) intentionally failed to report multiple security concerns/incidents involving A1C Teixeira as required. Had the SSO been properly notified, applicable regulations and instructions required actions including restricting systems and facility access, and alerting appropriate authorities, such as the DAF C-InT Hub or AFOSI to assess the potential insider threat. In addition, (b) (6), (b) (7)(C) likewise willfully failed to accurately and completely report the same pattern of security concerns and incidents to the SSO as required. 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 Title 10 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.

Observations

In addition to the direct contributing factors, a number of indirect contributing factors enabled the occurrence and duration of the improper collection and unauthorized release. These factors included:

- Inconsistent DoD and Air Force written guidance on reporting actual or suspected security incidents.
    - All responsible agencies should take action to clarify, consolidate, and standardize all written reporting guidance and instructions. Reporting should be made to both the command chain and the appropriate security official. Additionally, command and security should be required to verify notification to the other party as a crosscheck.
- Conflation of classified system access with the "need to know" principle, to include lack of robust validation of need to know.
    - All responsible agencies should take action to update written guidance and reemphasize the concept of verifying an individual's need to know for specific classified information within the digital domain.
- Lack of clarity and differing standards for need to know.
    - All responsible agencies should take action to update written guidance and reemphasize the responsibility for users with access to classified at any level to refrain from accessing information not required for their duties.
- Administrative/disciplinary action disparity between T32 and T10 members and lengthy processing times for administrative actions.
    - Responsible agencies should consider revisiting the T10 ADCON structure to either reduce the number of Airmen under the command, provide additional resources to manage the number of Airmen under command, or revise policy or law to ensure effective lower-level administrative actions for Airmen in T10 status.
- Lack of supervision and oversight during night shift operations.
    - All responsible agencies should ensure instructions, guidance, and business rules are implemented to limit extended periods of single person access to SAP and TS-SCI materials, and to validate or monitor classified printing.

- Unit personnel were not aware of potential areas concerns that arose from the SF-86 security screening process.
    - The SF-86 security clearance screening process should annotate potential areas of concern and ensure all recommendations for continued monitoring are proactively communicated to the unit.

As noted in the 3-8 May 23 Directed Inspection Report of the 102 ISRG, 102 IW leadership shall develop and implement a Corrective Action Plan to address the following observations:

- SCI material, INFOSEC Programs, and the IO Program lacking in key areas.
- Overall, Unit Self-Assessment Program (USAP) in disarray with significant pockets of dormant or non-existent programs.
- Culture of complacency in the 102 IW with respect to unit security reinforced risk-accepting behavior at inappropriate levels.

Conclusion

Three members in A1C Teixeira's supervisory chain willfully failed to report security related incidents to the SSO, and unit leadership failed to fully and effectively accomplish security program responsibilities. When combined with the other direct and systemic indirect contributing factors described above, these failures represent an overall lack of adherence to policy, procedures, and standards, and created a unit environment at the 102 IW that enabled and increased the opportunity for, and duration of, the unauthorized disclosure of national security information.

(b) (6), (b) (7)(C)

STEPHEN L. DAVIS
Lieutenant General, USAF
The Inspector General

LIST OF EXHIBITS

Exhibit