Inspector General Sensitive Information

The Inspector General of the Department of the Air Force

Directed Inspection on 102 ISRG, Otis ANGB MA 3-8 May 2023

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

Inspector General Sensitive Information

~~Controlled by: USAF~~
~~Controlled by: SAF/IG~~
~~Category: PRIIG~~
~~Limited Dissemination Control: DL ONLY~~
POC: AFIA [redacted]

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

Summary Report

Purpose
Report detailed results of the compliance and environment of the 102d Intelligence Wing (IW), Otis Air National Guard Base (ANGB), MA. Specifically, this report details the results of the Directed Inspection of the 102d Intelligence Surveillance, and Reconnaissance Group (ISRG) and includes the results of IG sensing sessions (IGS2) that assess the 102 IW culture regarding security and protection of classified information.

Background
This independent inspection was accomplished through a review of data provided by the organization, an on-site evaluation of specific programs, functional and leadership interviews, and sensing sessions of unit members. This inspection report summarizes on-site observations, group sensing sessions results, and provides recommendations for consideration in Appendices A - E.

Scope and Approach
Inspection activity was directed in the following three objectives:

a. Complete a full compliance inspection assessing processes and practices in the protection of classified materiel regarding sensitive compartmented information (SCI) and information security (INFOSEC) programs.
b. Complete a full Intelligence Oversight (IO) Program inspection.
c. Provide a preliminary assessment of Unit Self-Assessment Program (USAP) health.

The AFIA directed inspection (DI) team interviewed 40 personnel at 102 ISRG and subordinate squadrons, flights, and workcenters, analyzed current and proposed policy and procedures, and made observations relating to compliance of the objectives.

Inspector General Sensing Session Method
A tailored sensing session strategy was developed to assess the unit environment specifically for those conducting the intelligence mission. A total of 199 IGS2 participants were selected from the 102 IW, the 102 ISRG, and the 202 ISRG.

If you have any questions or concerns, please contact SAF/IG at DSN (b) (6), (b) (7)(C) or Comm (b) (6), (b) (7)(C)

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

STEPHEN L. DAVIS
Lieutenant General, USAF
The Inspector General

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

APPENDIX A

Objective 1
Complete a full compliance inspection assessing processes and practices in the protection of classified materiel regarding Sensitive Compartmented Information (SCI) and Information Security (INFOSEC) programs.

Conclusion
The INFOSEC and SCI programs were not in compliance with requirements.

Compliance Results
The 102 ISRG is supported by the 102 Intelligence Wing (IW) INFOSEC program, which lacked evidence of effective program activity prior to 2023. A concurrent review of several information security activities of the 102 ISRG SCI program revealed unclear delineation of responsibilities between the Special Security Officer (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 and resources to effectively accomplish remaining program responsibilities. Examples of resulting non-compliance included: local security instructions not meeting minimum requirements; inadequate maintenance of classified storage containers; ineffective exercise of Emergency Action Plan(s); poor enforcement of training requirements; and insufficient enforcement of proper classification markings.

These program deficiencies were coupled with a lack of INFOSEC inspection emphasis both by unit leadership and inspection activities. The October 2021 Air Combat Command Inspector General Unit Effectiveness Inspection did not identify any information security concerns. Furthermore, a security incident with resulting Commander Directed Investigation in February 2022 neither identified nor addressed broader INFOSEC issues. It was not until February 2023 that INFOSEC was identified as a significant program deficiency by the 102 IW Inspector General. The failure to identify and correct these deficiencies demonstrated a general lack of leadership emphasis, at all levels, on compliance with information security policy. Four deficiencies for this objective are detailed in Appendix D.

Sensing Session Results
Most unit members perceived that security practices at the 102 IW were "rigorous;" however, others noted that more robust practices were implemented at other locations with similar missions and levels of classification. Participants identified that security discipline was lax in areas such as members improperly displaying badges while on the Ops floor, leaving computer stations unlocked, and equating presence in the building with a clearance and a valid need-to-know. A contributing factor to acceptance of these practices was a high level of trust among members in the organization, resulting from long-term working relationships and knowledge that all members had appropriate-level clearance to be in the facility. Security-related training was described as

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

"constant" but not always effective as it was often considered no more than something to "check off" in order to return to mission activities.

Unit-Derived Recommendations

- Provide personnel a method to check and/or verify need-to-know. Although operations and requirements are dynamic, members found that long-term tenure at the unit creates a vulnerability to assuming need-to-know because a person has had it in the past. A visual indicator of current access requirements would enable the unit to police themselves.
- Conduct more frequent, small-scale security procedure exercises. These limited-scope events will help to ensure members can practice the appropriate reporting to notify all required POCs while reinvigorating the importance of security.
- Establish local trusted agent for issuing Public Key Infrastructure (PKI) certificates or oversight office to validate all PKI requests prior to submission. Currently, PKIs are issued by an organization external to Otis ANGB, which lacks the ability to validate appropriate requests or manage PKI status with personnel movements.
- Use small-group training sessions to discuss real world examples of security incidents and reporting procedures. This will help members understand the process and reporting requirements, bolstering wing-wide execution.
- Realign resources to increase on-site presence of leadership and security for mid-shift and swing-shift personnel.
- Seek opportunities to consolidate redundant training where credit for training on one system could be applicable to all systems. This may significantly reduce training fatigue and improve the use of Airmen's Time,

Inspector General Recommendations

- Clearly delineate security management roles and expectations between DIA, leadership, Chief of Information Protection, SSOs, and Security Managers. This would ensure that all positions are clearly aware of authorities and responsibilities in complying with the myriad of security regulations and any internal amplifying guidance.
- Review each member's access requirements and visually inspect each restricted area badge to ensure photos are recognizable.
- Air Combat Command Inspector General should schedule and conduct continual evaluation of 102d Intelligence Wing's INFOSEC and Intelligence Oversight responsibilities as outlined in DAFI 90-302 Attachment 3 within one year of publication of this report.

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee~~.

APPENDIX B

Objective 2
Complete a full Intelligence Oversight (IO) program inspection.

Conclusion
Intelligence oversight was acceptable but not fully in compliance.

Compliance Results
Inspection of the 102 IW IO program determined the program to be in compliance with notable exceptions. Numerous members of the 102 ISRG had not completed IO training; however, training materials were appropriately tailored to each mission's needs. Supervision did not facilitate reporting of known and possible IO-associated violations and irregularities to the 102 IW Inspector General and Staff Judge Advocate, or to unit-level IO monitors. Application of IO in the 102 IW did not consider IO's broader purpose, which includes reporting of Significant/Highly Sensitive Matters, regardless of whether the activity is unlawful. The unit's enforcement of compliance with IO was inconsistent. One deficiency for this objective is detailed in Appendix D.

Sensing Session Results
No overall trends were noted.

Inspector General Recommendations

- Develop practical exercises and questions to support members' understanding of IO requirements, significance, and procedures.
- Scrub the roles of assigned personnel, including physical location of work, to ensure all personnel who might encounter information on U.S. Persons in the course of their normal military duties as related to IO, are properly tracked for IO-training monitoring. This should include 102 IW Inspector General and Staff Judge Advocate.

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

APPENDIX C

Objective 3
Provide an assessment of the commander's inspection and Unit Self-Assessment Programs (USAP).

Conclusion
Existing inspection and self-assessment systems are inadequate.

Compliance Results
A well-communicated, actioned, and enforced self-assessment program was not evident across the majority of the 102 ISRG. Inspection data since 2020 showed known concerns and insufficient program improvement from wing, group, and squadron levels. Although intent from the 102 IW Commander and 102 ISRG Commander was codified in established business rules, subordinate commanders did not apply or enforce wing and group-level direction. Interviews with 102 ISRG personnel indicated a lack of awareness and understanding of the program at all levels. In their conversations with the inspection team, group and squadron program managers also suggested 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 Information Security and IO issues summarized in this memorandum. Two deficiencies for this objective are identified in Appendix D.

Sensing Session Results
The removal of the Standards and Evaluations function was noted in nearly every session as negatively impacting mission readiness. Although a quality-control function existed at the 102 ISRG level, this office also managed weapons and tactics as well as unit training. Furthermore, the training and quality control efforts were specific to the intelligence specialties and were not providing any training or oversight for cyber defense operations. Operations members are no longer certified by position or part of an ongoing quality assurance program. These issues highlight the result of an ineffective self-assessment program that did not extend beyond Management Internal Control Toolset checklists.

Inspector General Recommendations

- Incorporate a functional exercise of emergency action plans into self-assessment programs. Further, validation of those evaluations should be made an element of the 102 IW Commander's Inspection Program.
- Discontinue the practice of using a single office both to conduct training and to validate training through functional assessments. Keeping these roles together may skew the assessment of the quality of training and creates risk to miss training shortfalls.
- Establish a local by-position certification process to include both intelligence and cyber operations members.

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

- 102 ISRG Commander should provide clear intent for the group's self-assessment program as well as introducing the group and squadron self-assessment program managers at the next ISRG Commander's All-Call. Personnel should be provided with an overview of the program, how units can get involved, self-assessment techniques that can be used, and how to contact self-assessment leads for questions or concerns. Group and squadron program managers should continue to advertise to the unit periodically as a reminder to personnel of their responsibility to instill a culture of self-assessment within their work centers. Group and squadron program managers should update and utilize the ISRG's Self-Assessment Handbook and disseminate it to all personnel within the group.

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

APPENDIX D
Inspection Deficiencies

OBJECTIVE 1 - INFOSEC and SCI:

Tracking Number: F.135329.5470953
Severity: SIGNIFICANT
The 102 ISRG's security manager(s) failed to ensure personnel adhered to information security program requirements; specifically, 18 of 22 notebooks filled with derivatively classified working papers were not properly marked with the highest classification; did not include the date created, the person's name, or their position; and were not annotated as a working paper on each sheet.
Reference: 32 CFR vol B ch XX pt 2001 sub-pt F sec 2002.24 para (d) (T-0); DoDM 5200.01 vol 1 other Enclosure 2, para 8.b. (T-0), other Enclosure 3, para 13.b. (T-0), fig 11 (T-0); POTUS White House Executive Order 13526 sec 1.2. para (a)(1); POTUS White House Executive Order 13526 sec 2.1. para (b)(1)
Impact: Improper classification of these documents may result in improper handling of material which could reasonably be expected to cause exceptionally grave damage to the national security.

Tracking Number: F.135329.5471908
Severity: SIGNIFICANT
The 102 ISRG Special Security Officer (SSO) failed to establish and maintain an Emergency Action Plan (EAP) that met the requirements for all EAPs. Specifically, failed to:
- Combine EAP with host command's emergency plans (c)
- Provide for effective destruction in the event of an emergency (c)
- Practice EAP annually (d)
- Identify all materials for emergency destruction or removal by labelling f.(f)
- Designate alternates for duty position assignments (2)(b)
- Have all personnel conduct periodic review of assigned duties (2)(d)
- Identify location of SCI material by storage container (2)(e)
- Identify location of safe combinations (2)(f)
- Identify emergency storage procedures (2)(j)

Reference: DoDM 5105.21 vol 2 para 6.f.(1)(a) (T-0), para 6.f.(1)(c) (T-0), para 6.f.(1)(d) (T-0), para 6.f.(1)(f) (T-0), para 6.f.(2)(b) (T-0), para 6.f.(2)(d) (T-0), para 6.f.(2)(e) (T-0), para 6.f.(2)(f) (T-0), para 6.f.(2)(j) (T-0)
Impact: An EAP without these key elements puts the safety of Airmen and safeguarding of SCI material at risk during a crisis or emergency.

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee~~.

Tracking Number: F.135329.5471912
Severity: CRITICAL
The 102 ISRG Special Security Officer (SSO) critically failed to apply effective security management, operation, implementation, and oversee use of Sensitive Compartmented Information (SCI) material storage containers. Specifically:
- Multiple containers were missing opaque envelopes to house the SF 700, conspicuously marked "Security Container Information"
- A record of the names of persons having knowledge of the combination was not maintained and was not included in SSO's security management
- Custodians were not completing required inspections or performing/documenting combination changes whenever an individual knowing the combination to the container or vault door no longer requires access or when compromise of the combination may be suspected
- Did not ensure effort was focused on disposing of unneeded classified material at least once a year
- No efforts were made to segregate SCI material from other material in a separate file cabinet, drawer, or folder
References: DoDM 5105.21 vol 1 other Enclosure 2, para 9 (T-0); DoDM 5105.21 vol 1 other Enclosure 4, para 13.c. (T-0); DoDM 5200.01 vol 3 other Enclosure 3, para 10.a. (T-0); DoDM 5200.01 vol 3 other Enclosure 3, para 10.c. (T-0); DoDM 5200.01 vol 3 other Enclosure 3, para 11.a.(5) (T-0); DoDM 5200.01 vol 3 other Enclosure 3, para 11.b.(2) (T-0); DoDM 5200.01 vol 3 other Enclosure 3, para 17.b. (T-0)
Impact: The ineffective of management or oversight of SCI-storage containers could lead to mission impacts with working files unavailable for use by personnel executing time-sensitive missions. Further the lack of awareness of personnel access could allow personnel without need-to-know to access SCI material(s)

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

Tracking Number: F.135329.5470483
Severity: CRITICAL
The 102 IW/CC critically failed to provide information protection oversight through an information security program. Specifically, the program failed to:
- Ensure local security instructions, plans and/or processes included the minimum requirements identified
- [as SIO shall] Develop DoD Component-specific implementation guidance as necessary for the protection of Sensitive Compartmented Information
- Establish a Security, Education, Training and Awareness program
- Ensure 30 of 253 personnel who process classified information or utilize classified information systems had completed annual refreshers
References: DoDM 5200.01_DAFMAN16-1404 vol 1 para 7.n.(5)(a) (T-1), para 7.n.(7)(b) (T-1), para 7.n.(7)(c) (T-1), para 7.n.(7)(d) (T-1), para 11.(3) (T-0)
Impact: Long term failure of the program to provide adequate oversight of unit security programs and coordinated mitigation activities led to a deficient security culture which may have contributed to multiple significant security incidents.

OBJECTIVE 2 - INTELLIGENCE OVERSIGHT:

Tracking Number: F.135329.5471890
Severity: MINOR
The 102 IW Intel Oversight monitor did not provide 11 of 293 personnel initial and annual refresher training tailored to mission requirements.
Reference: DoDD 5148.13 para 2.4.c (T-0)

OBJECTIVE 3 - UNIT SELF-ASSESSMENT PROGRAM:

Tracking Number: F.135329.5471883
Severity: MINOR
The 102 ISRG/CC did not ensure a mandated Information Security Program Management Internal Control Toolset (MICT) checklist was part of the group's self-assessment program. This resulted in the Wing Chief, IP, not evaluating the effectiveness and efficiency of the support activities' information security program to include reviewing MICT checklists and communicating with wing leadership on the health of the information security program.
Reference: DoDM 5200.01 vol 1 ch 7 para 7.d.(4)(a) (T-1), para 7n(6)(b) (T-1)

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

Tracking Number: F.135329.5469861
Severity: CRITICAL
The 102 ISRG/CC critically failed to inspect their units and subordinates to ensure maximum effectiveness, efficiency, and discipline of the force were maintained in the areas of information security, sensitive compartmented information (SCI), and intelligence oversight. Specifically failed to:
- Put in place a robust self-assessment program that ensured appropriate internal mechanisms existed to track requirement and resource mismatches, assess resultant mission risk, and track disconnect to closure
- Establish and maintain an annual self-inspection and ongoing oversight program the ISRG's portion of the information security program pertaining to classified information
- Include regular reviews and assessments of representative samples of the ISRG's classified products (16-1404 Enc 2 para 7.d.(2))
- Oversee the protection of SCI through a comprehensive inspection program that includes self-inspections and random command/corporate-level reviews
- Adequately inspect intelligence oversight programs for compliance annually
- Conduct annual Personnel Security Program self-inspections, unit inspections, and metrics
Reference: AFI 1-2 para 3.4. (T-1); AFI 14-404 para 2.9.7. (T-1); AFI 16-1405 para 2.13.i.(6) (T-1), para 2.13.f.3. (T-1); DAFI 90-302 para 2.5.1. (T-0); DoDM 5105.21 vol 1 other Enclosure 2, para 7.c. (T-0); DoDM 5200.01 vol 1 other Enclosure 2, para 7.d. (T-0)
Impact: Lack of a USAP likely led to critical undetected non-compliance in Information Security (INFOSEC) and Intel Oversight (IO).

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

APPENDIX E
Sensing Session Details

Summary
Over a 10-day period, 87 full-time members were asked about the unit culture with respect to the unauthorized disclosure, collaboration policies, training and enforcement of security policies, and efforts to assess or validate security procedures. An additional 112 drill-status guardsmen (DSG) members were asked about the quality of security practices, members' understanding of reporting procedures, and for any suggestions for improving security practices.

The following is a summary of the participants' views about their respective organization. Summaries are reflective of personal opinions shared with facilitators and does not include IG validation.

FULL TIME MEMBER RESPONSE SUMMARIES:

FULL-TIME MEMBERS	
Category	**# Interviewed**
Airmen	8
NCO	40
SNCO	33
CGO	2
FGO	4
TOTALS	**87**

Question 1: Level of Surprise (1-10 rating)
Members typically indicated a high level of surprise that an unauthorized disclosure was possible given that expectations of security clearances and accesses were well-known. Also, policies were described as well-ingrained. Most members surveyed felt that the incident was shocking because anyone in the unit with a Top-Secret clearance would surely know not to reveal classified information and that there were consequences to doing so. They also emphasized the close-knit nature of the organization and level of trust that resulted from longtime associations. Most expressed that the possibility certainly existed for unauthorized disclosure from any source and that the threat can come from anywhere because it is nearly impossible to stop malicious intent. Responses focused on individual responsibility versus security practices to prevent incidents. Some members did indicate a lower level of surprise, in part due to the Ops floor layout and the lack of supervision on overnight shifts. Some also suggested that security practices were less stringent than other locations. However, most members perceived the level of security to be rigorous, even more so than other locations. Unit members still felt that it was "too close to home"

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

given the unit's overall morale, culture, and procedures/policies that they believed to be very positive in nature.

- Total Avg: 8.07 ("mostly surprised")
  - Amn Avg: 9.63 ("completely surprised")
  - NCO Avg: 7.58 ("somewhat surprised")
  - SNCO Avg: 8.27 ("mostly surprised")
  - CGO Avg: 8.50 ("mostly surprised")
  - FGO Avg: 8.00 ("mostly surprised")

Question 2: Collaboration and Communication (1-10 rating)

Members believed that there was always room for improvement with collaboration and communication but that generally all units worked well with each other to complete the mission, including timely responses for intelligence and information requests through proper channels. The 102d Intelligence Wing regularly communicated information via email and in-person briefings for a variety of scopes/intent, which groups and squadrons internally re-communicated as needed. Most members felt that units did a good job with keeping respective mission sets within their assigned "lanes," and there generally wasn't any real need or situation where crosstalk would occur unless there was a deliberate overlap and/or need-to-know. Members stated that tradecraft and basic Intelligence Community skills/practices were shared amongst those with the same AFSCs on a periodic basis through sync meetings. However, SNCOs and CGOs sampled expressed a level of frustration because they felt there is no effort by leadership or general "appetite" for the two SIGINT mission sets to collaborate, even on wing-level exercises.

Need-to-know for cross-group work was generally determined between the SSO and Cybersecurity section for both ISRGs, but the102 ISRG displayed a level of risk for "shoulder surfing" and inappropriate visibility of information on classified systems because of the open layout of the Ops floor. The IMOC (ISS work area) is near other units on the Ops floor, with no permanent physical barriers between the mission and support elements, allowing members to move between sections for collaboration and support. Additionally, the nature of the Intelligence Community relating to availability and access to restricted SIPRNET and JWICS websites/information is such that access requests (specifically for PKIs) are handled by a trusted agent unconnected to Otis ANGB who does not validate or coordinate approval with the requesting agency. The relationship between 102d ISS and 101 IS/102 OSS was described as more divided, due to the ISS system support function as opposed to working direct mission, unlike the 102 OSS and 101 IS. Leadership initiated efforts, such as providing intelligence briefs to ISS members, to include the ISS more with operations and to inspire members with their purpose. Fewer than 10 members of the 102 ISRG described some concerns and confusion regarding the content of these briefs weighed against need-to-know; however, squadron leadership had justified the events as a way for ISS members to understand their contributions. Approximately 15 full-time members from 102 ISRG indicated there was effectively no distinction between the 102 OSS and the 101 IS regarding mission responsibilities and execution. 102 ISS, 202 ISS, and 102 CF collaborated regularly specifically for system maintenance and troubleshooting and did not have a need to discuss classified

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

information or missions with each other. 102 CF did note that the ISS members often requested support on basic processes notably during night shift; it is unclear if they required assistance due to lack of training/experience, poor quality control procedures, or insufficient internal support on overnight shifts.

Total Avg: 7.37 ("good")
- Amn Avg: 8.25 ("very good")
- NCO Avg: 7.93 ("good")
- SNCO Avg: 6.70 ("somewhat good")
- CGO Avg: 3.50 ("poor")
- FGO Avg: 7.50 ("good")

Question 3: Training and Enforcement (1-10 rating for each)

As a whole, unit members felt that they received adequate training for both DAF and local security requirements on a regular basis, while acknowledging that the "ANG aspect" of their jobs meant unfamiliarity could develop without a self-controlled focus on maintaining proficiency (for those not on "full time") and that training was often monotonous and, at times, overwhelming because of the quantity required. The 102d Intelligence Wing appeared to place a heavy focus on a long drill weekend known as "March Madness" where the bulk of the annual requirements for members should be completed. Members felt that SSOs and other authorities regularly communicated security information and provided appropriate training on both a reoccurring and as-needed basis. Suggestions for improvement included more "practical application" and exercising of security measures, policies, and procedures by the SSO(s), IPO, and WIT to keep unit members engaged with cognitive engagement of this knowledge outside of CBTs and routine mission operations.

- Total Avg for **Training**: 8.31 ("very good")
  - Amn Avg: 9.13 ("almost perfect")
  - NCO Avg: 7.90 ("good")
  - SNCO Avg: 8.64 ("very good")
  - CGO Avg: 8.00 ("very good")
  - FGO Avg: 8.25 ("very good")

Most members believed that security and administrative measures are routinely aligned to prescribed standards and administered fairly across the unit, although there was a disagreement amongst FGOs in this respect because they felt the 102 ISRG SSO dealt with Enlisted members "more aggressively" for issues than the Officers. However, regarding enforcement, leaders appeared to favor verbal counseling for any disciplinary issues and treated MFRs as a "serious warning," believing that LOCs or higher should be reserved for blatant violations and repeat issues because of their perceived effect on promotion/hiring opportunities. It was not clear at what level of leadership the MFRs were reported to (or retained at), and a broad consensus of members surveyed reflected that this level of discipline was a "slap on the wrist." In general, most members expressed high confidence in their SSOs and Information Security Managers and felt comfortable

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

in reporting security concerns to them in addition to their own direct supervisor. There appeared to be a lack of clarity and consistency in responses regarding reporting procedures. Responses included to report to supervisor who would inform SSO, to contact SSO first, or to notify both SSO and supervisor. However, most respondents agreed that the SSO would be involved or notified of any security incident. It was unclear if these issues were always reported to the SSO or if supervisors generally exercised a degree of discretion in determining what should be reported. Some members stated that this process of not going directly to the SSO for security issues (except for personal issues such as divorce) was "part of their training," but this could not be validated or substantiated.

- Total Avg for **Enforcement**: 8.31 ("very good")
  - Amn Avg: 8.75 ("very good")
  - NCO Avg: 8.03 ("very good")
  - SNCO Avg: 8.48 ("very good")
  - CGO Avg: 9.50 ("almost perfect")
  - FGO Avg: 8.25 ("very good")

Question 4: Validation and Testing (no rating)
Confidence in validation and testing for security policies/procedures varied from unit to unit, and not all members gave a majority consensus for internal assessment specifics, which could partly be attributed to time on station variances and the differences in shift schedules for members surveyed. Some respondents noted that a wide variety of random checks were accomplished, including bag/pocket checks and Bluetooth signal sweeps, while others couldn't recall a single instance of a random check being done in the recent past. Most units did not articulate any QA functions or programs for security aside from those completed on a purely functional basis. Members expressed that these checks are usually driven by an individual SSO's preferences rather than any defined local policies. Almost all members stated that it was rare to see any after-action reports or documentation for security validation activities, and they were not aware of any after-actions taken aside from an "reminder" email being sent if a finding was serious or particularly noteworthy or if there was a trend identified for security issues.

DRILL-STATUS GUARDSMEN (DSG) RESPONSE SUMMARIES:

DSG MEMBERS	
Category	**# Interviewed**
Airmen	36
NCO	44
SNCO	19
CGO	6
FGO	7
TOTALS	**112**

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

Question 1 – Security Practices of the Unit

Members mostly rated the security practices of the wing highly. As in the sessions with the full-time military members, DSG participants highlighted the amount of training they received; some acknowledged that the training methods (i.e. CBTs and large group briefings) were not as effective. Repetition was seen as both a positive – members had the information ingrained due to completing the training so many times – as well as a negative – decreased importance and complacency because training was merely a "checkbox" to return to mission. Comments also acknowledged that security discipline could be lax; the level of trust in the organization led to unbadged members not being challenged and computers left unlocked with the request or expectation that coworkers would "keep an eye" on the station. For the 102 ISRG, facial recognition and presence on the Ops Floor were sufficient reasons to trust a member's access/clearance. In the 202 ISRG, more physical barriers prevent members from access to mission activity unless authorized. Other gaps in security practices included lack of positive control over material, "piggybacking," unnecessary PKI access, inability to assess/verify need-to-know, and unclear or multiple guidance sources that could be interpreted differently. Members did note a culture of "self-policing" where they would remind each other about reporting factors to the SSO, maintaining OPSEC, and completing training to maintain mission access.

Total Average for **Security Practices**: 7.98 ("good")

- Amn Avg: 8.08 ("very good")
- NCO Avg: 7.86 ("good")
- SNCO Avg: 7.89 ("good")
- CGO Avg: 8.5 ("very good")
- FGO Avg: 8 ("very good")

Question 2 – Incident Reporting

Members believed they understood incident reporting well but were uncertain as to what occurred after a report had been made. As with the full-time members, a majority of DSG participants indicated they would feel comfortable reporting concerns to the SSO or asking for clarification. If they had concerns, participants noted they might seek out direct supervisors, crew leads, or more senior-ranking members but were uncertain about the severity or what would meet the threshold that would require reporting. Most participants noted they had had little practical experience or exposure to reporting security concerns or incidents. Their knowledge was exclusively the result of the trainings, either via CBT or mass trainings during "March Madness." Participants indicated that the lack of practical application or experience meant they would be unsure about addressing an incident should it occur. DSG members also indicated that they dedicated all drill time to training and were not working missions; all training was given the same level of importance and the message from leadership was to ensure all items were checked off so they could perform mission, despite insufficient time to work mission. Members did

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee~~.

highlight concerns regarding overnight shifts as there is not a full-time SSO for the 24-hour facility. When an SSO was not present, members felt comfortable discussing concerns with their own supervisors; some also indicated that their personal responsibility ended by notifying a supervisor of concerns.
Total Average for **Understanding Incident Reporting**: 7.87 ("good")

- Amn Avg: 8.11 ("very good")
- NCO Avg: 7.48 ("good")
- SNCO Avg: 8.21 ("very good")
- CGO Avg: 7.67 ("good")
- FGO Avg: 8.29 ("very good")

Question 3 – Suggestions
In addition to those mentioned in the Objective Conclusions (Appendices A-C), members offered the following suggestions and requests for improving security practices:

1. Physical redesign of 102 ISRG Ops floor, to include relocating the IMOC off the floor
2. More robust printing management, such as:
    a. Restricting accounts for printing ability
    b. Physical restriction of printers
    c. Two-person tracking of printed material
    d. Verification of shredding for printed material
3. Restricting opaque bags from the Ops floor

All members (AGR/Technicians/DSG) were given the opportunity to provide additional comments (not limited to security)

- Members praised leadership as being connected, well-informed, and caring about their people. Members praised the culture, describing the unit as "their family" and noting the positive relations and high levels of trust due to many years of working with the same people. Enthusiasm for the mission was also high for the full-time members; DSG members noted little mission time due to focus on training during drill.
- Physical security of the base was a concern due to Security Forces manning, no security presence in the secured facility, and leadership not emphasizing importance of drills such as Active Shooter Exercises.
- Members suggested leadership and management did not value physical fitness as much as they should and wanted it reintegrated into the unit culture.
- Morale was high, but shift work made unit-wide events challenging to plan.

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

APPENDIX F
Key Personnel

POSITION	***NAME***	***RANK***	***DSN***	***~~EMAIL~~***
Team Chief	Stephen L. Davis	Lt Gen	[redacted]	[redacted] (b) (7)(C)
Inspector	[redacted]	[redacted]	[redacted]	(b) (6), (b) (7)(C)
Inspector	[redacted]	[redacted]	[redacted]	(b) (6), (b) (7)(C)
Inspector	(b) (6), (b) (7)(C)	[redacted]	[redacted]	(b) (6), (b) (7)(C)
Inspector	[redacted]	[redacted]	[redacted]	(b) (6), (b) (7)(C)
Inspector	(b) (6), (b) (7)(C)	[redacted]	[redacted]	(b) (6), (b) (7)(C)
Inspector	(b) (6), (b) (7)(C)	[redacted]	[redacted]	(b) (6), (b) (7)(C)
Inspector	(b) (6), (b) (7)(C)	[redacted]	[redacted]	(b) (6), (b) (7)(C)
Inspector	[redacted]	[redacted]	[redacted]	(b) (6), (b) (7)(C)
Inspector	[redacted]	[redacted] t	[redacted]	(b) (6), (b) (7)(C)
Pertinent Oversight Authority: AF-A2/6UZ	(b) (6), (b) (7)(C)	[redacted]	[redacted]	(b) (6), (b) (7)(C)

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

APPENDIX G
Acronyms

AFI – Air Force Instruction
AFIA – Air Force Inspection Agency
AFSC – Air Force Specialty Code
ANGB – Air National Guard Base
CBT – Computer Based Training
CF – Communications Flight
CFR – Code of Federal Regulations
CGO – Company Grade Officer
DAFI – Department of the Air Force Instruction
DAFMAN – Department of the Air Force Manual
DI – Directed Inspection
DIA – Defense Intelligence Agency
DoD – Department of Defense
DoDM – Department of Defense manual
DSG – Drill-Status Guardsmen
DSN – Defense Service Network
EAP – Emergency Action Plan
FGO – Field Grade Officer
IGS2 – Inspector General Sensing Session
IMOC – Integrated Mission Operations Center
INFOSEC – Information Security
IO – Intelligence Oversight
IP – Information Protection
IPO – Information Protection Office
IS – Intelligence Squadron
ISRG – Intelligence Surveillance & Reconnaissance Group
ISS – Intelligence Support Squadron
IW – Intelligence Wing
JWICS – Joint Worldwide Intelligence Communications System
LOC – Letter of Counseling
MFR – Memorandum for Record
MICT – Management Internal Control Toolset
NCO – Non-Commissioned Officer
OPSEC – Operational Security
OSS – Operations Support Squadron
PKI – Public Key Infrastructure
POC – Point of Contact
POTUS – President of the United States
QA – Quality Assurance
RIA – Recommended Improvement Area

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee.~~

SAF/IG – Air Force Inspector General
SCI – Sensitive Compartmented Information
SecAF – Secretary of the Air Force
SIGINT – Signals Intelligence
SIPRNET – SECRET Internet Protocol Router Network
SNCO – Senior Non-Commissioned Officer
SSO – Special Security Officer
USAF – United States Air Force
USAP - Unit Self-Assessment Program
WIT – Wing Inspection Team

~~This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside of the inspector general channels without prior approval of The Inspector General (SAF/IG) or designee~~.