



(U) Results in Brief

(U) Followup to DODIG-2018-068, "Evaluation of Oversight of Privileged Users Within the Army's Intelligence Component"

(U) June 19, 2019

(U) Objective

(U) We determined whether the U.S. Army Intelligence and Security Command (INSCOM) implemented the recommendations to improve controls over Joint Worldwide Intelligence Communications System (JWICS) privileged users in response to Report No. DODIG-2018-068, "Evaluation of Oversight of Privileged Users Within the Army's Intelligence Component," January 30, 2018.

(U) Background

[REDACTED]

The report included two recommendations to address the deficiencies identified during the evaluation. Recommendation 1 was issued to the Commander of U.S. Army Cyber Command to complete and execute the "Army User Activity Monitoring Program Concept of Operations." Recommendation 2 was issued to the INSCOM Chief of Staff and included four sub-parts. Specifically, we recommended that INSCOM:

- a. (U) Complete and execute INSCOM Policy 6-3 to define the authorities, program oversight and governance, and to ensure a cybersecurity audit process is in place prior to the transfer of user activity monitoring responsibilities to U.S. Army Cyber Command;

(U) Background (cont'd)

- b. (U) Enhance controls and processes to ensure that all records in Army Training and Certification Tracking System (ATCTS) are complete, accurate, and properly reviewed to comply with DoD instructions and Army regulations;
- c. (U) Review privileged users, enter all missing records into ATCTS, and correct all errors in ATCTS records; and
- d. (U) Revalidate all privileged users to ensure that access is commensurate with current mission requirements, and promptly revoke privileged access from any user who no longer requires such access.

(U) The Commander of U.S. Army Cyber Command and the INSCOM Chief of Staff agreed to take actions to close the two recommendations in Report No. DODIG-2018-068. We considered Recommendation 1 to U.S. Army Cyber Command resolved, and Recommendations 2.a and 2.b to INSCOM closed prior to initiating this followup.

(U) Finding

(U) We determined that INSCOM's actions to implement Recommendations 2.c and 2.d did not improve controls over ATCTS records and privileged users, because:

- [REDACTED]



(U) Results in Brief

(U) Followup to DODIG-2018-068, "Evaluation of Oversight of Privileged Users Within the Army's Intelligence Component"

(U) Finding (cont'd)

- [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(U) Management Comments and Our Response

(U) The INSCOM Chief of Staff agreed with our recommendations. INSCOM distributed "INSCOM ATCTS Tactics, Techniques and Procedures" and examples of each required ATCTS form detailing actions. INSCOM stated that ATCTS managers will perform joint quarterly reviews and daily ATCTS profile management. INSCOM also developed ATCTS training and has scheduled training sessions to ensure that ATCTS managers across the command are aware of their roles, responsibilities, and requirements as ATCTS managers in accordance with established guidance. In addition, INSCOM revised the current privileged user compliance dashboard to accurately reflect ATCTS documentation and quarterly review compliance across the command. The Ground Intelligence Support Activity-Bragg developed an online tool, the pilot for which was planned to commence on June 1, 2019, to standardize the System Authorization Access Request, Acceptable Use Policy and Privileged Access Agreement for the command. The web portal tool will maintain a repository of all INSCOM and non-INSCOM JWICS account documentation in Ground Intelligence Support Activity-Bragg.

(U) Recommendations

(U) We recommend that the INSCOM Chief of Staff:

- (U) Develop a plan for ATCTS managers to conduct quarterly reviews of privileged users as required by DoD and Army guidance.
- (U) Develop tools that capture all information required in training and nomination records, and report accurate information matching the records in ATCTS to verify privileged user compliance with DoD and Army guidance.

(U) Comments from the INSCOM Chief of Staff addressed the specifics of the recommendations; therefore, the recommendations are resolved, but will remain open. We will close the recommendations once we verify that ATCTS managers are conducting quarterly reviews of privileged users as required, that the online web portal is operational, and that the revised dashboard accurately reflects privileged user compliance. Please see the Recommendation Table on the next page for the status of recommendations.

(U) Recommendations Table

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief of Staff, U.S. Army Intelligence and Security Command	None	1.a, 1.b	None (U)

(U) Note: The following categories are used to describe agency management’s comments to individual recommendation:

- **(U) Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **(U) Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **(U) Closed** – OIG verified that the agreed upon corrective actions were implemented.