National
INSIDER THREAT
Task Force

ADVISORY: Maturing the Enterprise - *Insider Threat Overlays*

NITTF - ADV– 2019 – 001

DATE: 5 September 2019

PURPOSE:

The National Geospatial-Intelligence Agency's (NGA) information security and insider threat programs developed the attached guide, the *Insider Threat Overlays* (*Overlays*), to provide a single, standardized source that integrates and synchronizes universal cybersecurity practices and risk management framework (RMF) methodologies with insider threat requirements and best practices. The *Overlays* expands upon insider threat controls highlighted in National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix G,[1] and provides a detailed roadmap for configuring information assurance controls to best support counter insider threat efforts. To aid department and agency consideration of its adoption and implementation, separate security control baselines have been developed to guide IT system owners, common cybersecurity solution providers, and insider threat programs to work together to maximize the relevant security controls. The *Overlays* provides control selection justifications, describes control extensions focusing on insider threat, provides a risk statement and supplemental guidance in the implementation of the control, and identifies specific references related to each control.

GUIDANCE:

The NITTF recommends Departments and Agencies adopt the *Insider Threat Overlays* as a crucial step toward organizational maturity. Maturity Framework Element 3 highlights the importance of adapting to changes in law, policy, organizational structure, and IT architecture. By adopting the *Overlays*, organizations can further strengthen the relationships between traditional cybersecurity practices and their dedicated insider threat program efforts to enhance their ability to deter, detect, and mitigate insider threats.

[1] http://csrc.nist.gov

BACKGOUND:

In November 2018, the NITTF released the *Insider Threat Program Maturity Framework* (*Framework*),[2] building upon the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (the *Minimum Standards*). Several Framework elements promote an enterprise approach to countering insider threat through integration of insider threat objectives with organizational missions and functions,[3] and ensuring insider threat programs continue to evolve and adapt to changing laws, policies, organizational structure, and information technology (IT) architecture.[4]

Consistent with the spirit of the *Framework*, the *Overlays p*rovides guidance for Information Assurance (IA) and insider threat professionals to work together to maximize both IA and insider threat requirements. Section G.1.b of the *Minimum Standards* requires insider threat programs have access to all relevant network information generated by IA elements. A separate requirement from user activity monitoring (Section H.1), this standard draws upon enterprise audit capabilities across all networks, both classified and unclassified. NIST and the Committee for National Security Systems (CNSS) have provided detailed guidance on information security controls for network security. Combined with the detail in the *Overlays*, these controls can greatly improve insider threat detection capability.

NITTF POC: Queries about this advisory should be directed to NITTF-TECHNICAL@dni.gov.

R. Wayne Belk

R. Wayne Belk
Co-Director (ODNI)
National Insider Threat Task Force

[2] https:// www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf

[3] NITTF Insider Threat Maturity Framework, November 2018, Maturity Element 1 states that insider threat programs should "exist as a dedicated effort, positioned in the D/A (Department or Agency) to ensure access to leadership to build support, and integrate insider threat objectives within the D/A's mission and function."

[4] Maturity Framework Element 3.