# Insider Threat Program (InTP) Maturity Framework
# Frequently Asked Questions (FAQs)

*What is the Maturity Framework (Framework) designed to do?*

**Answer:** The "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," (November 21, 2012) provide executive branch departments and agencies (D/As) with the **minimum** elements necessary to establish functional insider threat programs (InTPs); therefore, the Minimum Standards serve as milestones in the InTP maturity process. To help prevent the compromise of sensitive or classified information and to protect the resources and capabilities of the US Government (USG), InTPs must continue to enhance their policies, processes, methodologies, and capabilities. The Framework is designed to help programs evolve beyond the Minimum Standards to become more proactive, comprehensive, and better postured to deter, detect, and mitigate insider threat risk.

*How was the Maturity Framework developed?*

**Answer:** As part of its assigned responsibilities under Executive Order (EO) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," (October 7, 2011) and the National Policy and Minimum Standards, the National Insider Threat Task Force (NITTF) is charged with reviewing, and, if appropriate, adding to or modifying the Minimum Standards and guidance, in coordination with executive branch D/As. Beginning in the Fall of 2017, NITTF held a series of working groups to solicit ideas from the USG Insider Threat Community. Based upon the feedback received in the working groups, NITTF then developed a draft framework, modeled on the capability maturity model (CMM) process improvement approach used in industry. The resulting framework was vetted through a series of NITTF-hosted focus groups held throughout the Spring of 2018 that included representatives from Intelligence Community, Department of Defense, and Federal Partner insider threat programs.

*Why did NITTF decide to use a Framework format instead of Standards?*

**Answer:** The Minimum Standards established a baseline of capabilities for all InTPs within the USG Insider Threat Community. Over time, armed with the body of knowledge gleaned through the independent assessment process, NITTF recognized that beyond this baseline, each D/A must be allowed to mature its capabilities to assess and mitigate the threats from within their unique environment. New standards applicable to all would take away flexibility and replace it with a one-size-fits-some solution. The Framework construct allows D/As to choose among the maturity elements for those that best fit with their workplace environment, technology infrastructure, and mission.

*Why introduce the Framework now, when many D/As are still working to achieve Minimum Standards Full Operating Capability (FOC)?*

**Answer:** Achieving FOC is not a prerequisite for employing elements of the Framework. Those programs that are close to FOC will benefit from the increased capabilities gained through implementation of Framework elements. For other programs, the challenges they face in achieving FOC will likely require additional effort and resources to overcome. The elements of the Framework will help sharpen their ability to identify and mitigate possible insider threat risk while they continue to address those challenges.

*Does the Framework replace the Minimum Standards?*

**Answer:** No. The Minimum Standards must still be met. Executive branch D/As subject to EO 13587 must still comply with the National Policy and Minimum Standards. The Framework provides guidance for maturing programs beyond the minimum requirements.

*Is the Framework a new set of standards for InTPs?*

**Answer:** No. The Framework identifies key elements within the existing Minimum Standards construct that when enhanced, enable D/As to increase the effectiveness of program functionality, garner greater benefit from InTP resources, procedures, and processes, and tightly integrate InTP goals and objectives with their D/A's missions and challenges. Each element within the Framework has been identified as a capability or attribute exhibited by an advanced insider threat program. However, each D/A should evaluate the applicability of Framework elements to their environment.

*Are D/As required to implement the Framework elements?*

**Answer:** No. The Framework is a general blueprint for D/As as they seek to advance their InTP's capabilities and evolve beyond the Minimum Standards. When using the Framework, D/As should employ risk management principles tailored to meet the needs of their workplace environment, technology infrastructure, and mission. InTPs must also ensure compliance with their D/A's policies, regulations, and all applicable legal, privacy and civil liberties, and whistleblower protections when evaluating and incorporating Framework elements.

*Is there a timeframe or deadline for InTPs to implement Framework elements?*

**Answer:** No. InTPs should review the Framework and assess which elements might be appropriately incorporated into their program in consultation with their D/A's Office of General Counsel (OGC), Office of Inspector General (OIG), and privacy and civil liberties officials. Once a determination has been made on the element(s) to be incorporated, InTPs may wish to develop a program of action and milestones to help facilitate implementation of the Framework element(s).

*Will InTPs be assessed against the Framework elements?*

**Answer:** Since the Framework is not a new set of standards, InTP implementation of maturity elements (MEs) will not be formally assessed. However, the NITTF will note during an independent assessment when an InTP has incorporated MEs into its program construct and documentation. NITTF is gathering best practices that can be used throughout the USG Insider Threat Community to help other programs mature and optimize their capabilities. As the National InTP matures its overall effectiveness through these best practices, many of which can be found in the Framework, the NITTF will evolve its assessment process to include measures of effectiveness.

*How can an InTP use the Framework?*

**Answer:** InTPs can use the Framework as a roadmap to develop strategic goals and objectives to evolve their capabilities, processes, procedures and resources to meet current **and** future challenges in countering the insider threat. InTPs should also incorporate considerations for their unique D/A mission, workforce environment, and technology infrastructure as they develop their course of action and implementation plans. Additionally, InTPs should engage their OGC, privacy and civil liberties officials, and OIG early on in their planning process to ensure what is developed complies with all applicable legal, privacy and civil liberties rights, and whistleblower protections.

*What assistance is available to a D/A in implementing the Framework?*

**Answer:** The NITTF is prepared to provide continued support, advice and assistance, not only as D/As continue to implement the Minimum Standards but also as their InTPs begin to employ the Framework. As with efforts to develop programs to date, the resources to implement the elements of the Framework will be the responsibility of the individual D/As. The NITTF stands ready to offer best practices as well as introductions to other D/A programs that may have the information programs need to move forward.

*My D/A is small/has a small number of cleared employees/not much access to classified information. How does the Framework apply to my InTP?*

**Answer:** Unlike the Minimum Standards, which require that all specified requirements be met, the Framework is specifically designed to give D/A's the flexibility to implement the MEs the D/A sees as beneficial to enhancing the capabilities of its InTP.