Full Operating Capability

An executive branch insider threat program reaches Full Operating Capability (FOC) by implementing all 26 of the Minimum Standards. An insider threat program at FOC:

- Understands that detecting, deterring, and mitigating insider threats is a human-centric endeavor, focusing on human behavior.
- Operates in a proactive posture, and seeks to identify anomalous behaviors and intervene to prevent an insider from using their authorized access, wittingly or unwittingly, to do harm to the security of the United States.
    - The goal is to intercede with an employee before a crisis occurs, and get the employee the help or assistance they need so they can remain an employee of the organization in good standing.
- Receives strong and active support from the organization head and the designated senior official (DSO).
- Has a DSO with direct access to the organization head on insider threat matters and who is high-ranking enough to communicate as a supervisor or peer with organizational data-holding component leadership.
- Produces approved foundational documents that have been reviewed by general counsel and civil liberties and privacy officials.
    - Ensures the proper authorities to conduct program business and that activities are legal and respect employees' rights.
- Produces approved processes and procedures, and institutes technical mechanisms to strictly limit access to records and data created as a result of authorized program activities.
    - Program personnel have access to vast amounts of sensitive, personally identifiable information that must be protected.
- Trains program personnel in multiple disciplines, but those personnel are discipline-agnostic.
    - Ensures reported anomalous behaviors receive the broadest examination possible to properly contextualize them.
    - Ensures program personnel gain, maintain, and continuously hone the knowledge, skills, and abilities to properly conduct program activities.
- Has authorized access to multiple internal and external data sources, to include sensitive data sources, information derived from monitoring of users' activities on all classified computer networks, and information assurance data from classified and unclassified computer networks.
    - Under reactive circumstances, allows program personnel to pull germane data streams into the program for resolution of a specific matter.
    - Under proactive circumstances, data holders automatically push pre-determined trigger events to the program, so that matters can potentially be linked over time.
- Maintains an insider threat hub, where trained personnel, using approved processes, procedures, and guidelines, and with authorized access to multiple data streams, puts anomalous behavior into context, and makes a determination of the necessity to refer a matter to a proper mitigation authority.
- Creates a culture of awareness about insider threats for all cleared employees through training and awareness campaigns, and by providing ample information for the workforce on an easily found network site that includes a secure way to contact the program.
    - Training and awareness helps employees understand that the primary purpose of an insider threat program is to protect classified information.
    - Secondarily, robust programs also protect employees and their workplaces.
    - Ideally includes all of an organization's employees, both cleared and uncleared.