DEPARTMENT OF JUSTICE

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Insider Threat Minimum Standards

D		F		G		H		E		I	
Designation of Senior Official		**Insider Threat Personnel**		**Access to Information**		**Monitor User Activity on Networks**		**Information Integration, Analysis, and Response**		**Employee Training and Awareness**	
1 P	Designate a senior official	1	Program personnel trained in CI and security fundamentals	1	Program receives timely relevant component information – CI and security, IA, and HR	1	Monitor user activity on at least one classified network	1	Build and maintain an insider threat analytic and response capability to ingest, review, centrally analyze, and respond to internal relevant information	1	Create procedures for initial and recurring training for employees to include documentation
2 P	Develop an insider threat policy	2	Program personnel trained in conducting response actions	2 P	Establish procedures for program personnel to access to sensitive or protected information		Monitor user activity on all classified networks, either via internal or external agreements	2 P	Establish procedures for insider threat response actions – centrally managed by the insider threat program	2	Verify all cleared employees have completed insider threat awareness training
3 P	Establish an implementation plan	3	Program personnel trained in gathering, integration, retention, safeguarding, and use of records and data	3 P	Establish reporting guidelines for component departments to refer relevant insider information	2 P	Create policies for protecting, interpreting, storing, and limiting access to user activity monitoring methods and results	3 P	Develop procedures for documenting each matter reported and response action taken	3	Establish and promote an internal network site with insider threat information and secure reporting means
	Produce an annual report	4	Program personnel trained in applicable civil liberty and privacy laws	4	Program has timely access to CI reporting and analytical products pertaining to adversarial threats	3	Obtain signed agreements by all cleared employees				
4	Coordinate program activities with proper authorities – OGC/CLPO	5	Program personnel trained in 811 referral requirements and other applicable policy or statutory investigative referral requirements			4	Ensure there are classified and unclassified network banners informing users that networks are monitored				
5 P	Establish records handling and use procedures										
6 P	Establish records retention guidelines										
7	Facilitate oversight reviews for policy and legal compliance										

Program Establishment
Initial Operating Capability
Full Operating Capability

P = Written guidance required

A comprehensive program tracks, collects, and analyzes information to identify anomalous behavior in order for departments and agencies to deter, detect, and mitigate insider threats.