Cross Agency Priority Goal
Quarterly Progress Update

Insider Threat and
Security Clearance Reform

Goal Leaders:

Andrew Mayock, Senior Advisor to the Director,

Office of Management and Budget;

James Clapper, Director of National Intelligence;

Beth Cobert, Acting Director, Office of Personnel Management;

Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator

FY2016 Quarter 3

Overview

Goal Statement

Promote and protect our nation’s interests by ensuring aligned, effective, efficient, secure, and reciprocal vetting processes to support a trusted Federal workforce.

Urgency

Our world is changing at a pace that requires the security, suitability/fitness, and credentialing (SSC) community to anticipate, detect, and counter both internal and external threats, such as those posed by trusted insiders who may seek to do harm to the Federal government’s policies, processes, and information systems.

Vision

A Federal workforce entrusted to protect U.S. Government information and property; and to promote a safe and secure work environment, sustained by an enhanced risk management approach supported by:

- Improved early detection enabled by an informed, aware, and responsible Federal workforce
- Quality decisions enabled by improved investigative and adjudicative capabilities
- Optimized government-wide capabilities through enterprise approaches
- Insider Threat Program seeking to deter or mitigate problems before they negatively impact the workforce or national security

Re-baseline Overview

Over the past decade, we have established a firm foundation for Executive branch-wide SSC reform efforts, which have been essential to driving the implementation of key reform milestones:

- EO 13467 created the Suitability and Security Clearance Performance Accountability Council (PAC), the Security Executive Agent (SecEA), and the Suitability Executive Agent (SuitEA), establishing a strong leadership and solid governance structure for alignment and oversight.
- The 2012 Federal Investigative Standards is a tiered investigative model that provides consistent processes across the Executive branch and advancements in reciprocity.
- Key reform enabling organizations ensure accountability by agencies and achieve the goals of reform (i.e., the PAC Program Management Office (PMO), the Enterprise Investment Board (EIB), and SSC Line of Business (SSCLoB).

An Executive branch and enterprise-wide strategy was necessary to guide ongoing SSC reform efforts and sustain reform momentum, especially to ensure that we took a holistic, proactive approach instead of one where the government reacted to adverse events.

Thus, pursuant to the recent PAC cross-agency review undertaken in July 2015 to re-examine SSC reform efforts and determine whether further improvements could be made to the way the Government conducts SSC background investigations (and consistent with Government Accountability Office (GAO) recommendations, legislative mandates, and other reviews), the PAC issued the PAC Strategic Intent and Enterprise Information Technology (EIT) Strategy to outline our five-year business and technical vision.

Re-baseline Overview (cont.)

The Insider Threat and Security Clearance Reform (ITSCR) Cross Agency Priority (CAP) Goals have been re-baselined so that they are aligned with the new enterprise-wide focus of the PAC Strategic Intent and EIT Strategy, and its four work streams **(Trusted Workforce, Modern Vetting, Secure and Modern Mission-Capable IT, and Continuous Performance Improvement)** for modernizing the SSC mission over the next five years.

The CAP Goal milestones that are still outstanding or in progress have been incorporated into the rebaselined report as either key milestones or lower level milestones that will be tracked through this Quarterly Progress Update. We will still continue to report progress on these lower level milestones through the Key Highlights section.

The SSC mission, which is the responsibility of many diverse agencies across the Federal Government, continues to face implementation challenges. While these challenges are not insurmountable, they do require monitoring and regular re-assessment to sustain agency attention and dedication of appropriate resources. Accordingly, the PAC, with its interagency partners, will review the roadmap and its key milestones on an annual basis to reassess and reprioritize based on emerging needs and evolving threats.

Key Progress Highlights (FY16 Q3)

Trusted Workforce

We must equip our workforce with the necessary training and resources to assist the workforce in responsibly reporting and/or self-reporting information of potential concern.

- Establishing consistent requirements and protocols for handling and protecting reported information is a key step to improve the Federal workforce's confidence that the information will be properly safeguarded. The Security Executive Agent will soon finalize Security Executive Agent Directive (SEAD) 3, which provides aligned and standard reporting requirements for the Federal government.

Modern Vetting

We must modernize our SSC vetting policies, processes, and workforce to reduce waste, increase quality, enhance effectiveness, and improve efficiency.

- The May 2016 Security Executive Agent Directive (SEAD) 5 permits agencies to collect and evaluate valuable publicly-available social media information as part of vetting for national security eligibility.
- To improve background investigation quality, we must begin by measuring. In April 2016, the Executive Agents approved the government-wide investigative Quality Assessment Standards (QAS) Implementation Memorandum and Plan, which will enable implementing the QAS across the federal government.
- Determining the appropriate sensitivity designation for the government's national security positions will enable agencies to effectively manage risk and realize efficiencies by ensuring that positions are investigated at the right risk level. In May 2016, the Executive Agents issued implementation guidance for 5 CFR 1400, "Designation of National Security Positions in the Competitive Service, and Related Matters" that provide uniform and consistent guidance and procedures for position sensitivity designations.

Key Progress Highlights (FY16 Q3)

Secure and Modern Mission-Capable IT

We must secure the end-to-end environment, enhance SSC IT systems, establish SSC end-to-end shared services, and treat SSC data as a shared asset to support aligned, modern, and secure SSC IT systems and data.

- In today's environment, leveraging automation and technology, while protecting against internal and external threats to the security of data must be a high priority. DoD has identified IT and security requirements for a new and modern "eApplication" system, which will replace OPM's current application system (electronic Questionnaire for Investigations Processing (eQIP)).
- As part of the PAC Security and Suitability Review undertaken to modernize and strengthen the way we conduct background investigations for Federal employees and contractors and protect sensitive data, a National Background Investigations Bureau (NBIB) Transition Team was created to stand up the NBIB in October 2016, and has partnered with DoD to enhance the security of existing OPM IT systems and established processes to design a new NBIB IT system.

Continuous Performance Improvement

We must establish a continuous performance improvement model and institutionalize outcome-based performance metrics to identify and drive enterprise-level enhancements to policy, oversight, and operational processes.

- With diverse agencies in the SSC community, creating a unified vision and mission is vital to reform success. In July 2016, the PAC Principals signed the PAC Strategic Intent, which established a unified five-year strategic vision across the SSC mission and sets forth an objective to implement and continuously re-evaluate outcome-based metrics that measure the effectiveness of the SSC mission.
- Once goals have been identified, a comprehensive implementation plan will be put in place that guides the PAC, Executive Agents, and key stakeholder agencies to accomplish those goals. The PAC Implementation Plan finished informal coordination in August 2016, which will establish a streamlined cross-agency plan and roadmap to achieve the PAC strategic goals.

Key Progress Highlights (FY16 Q3)

Insider Threat Program

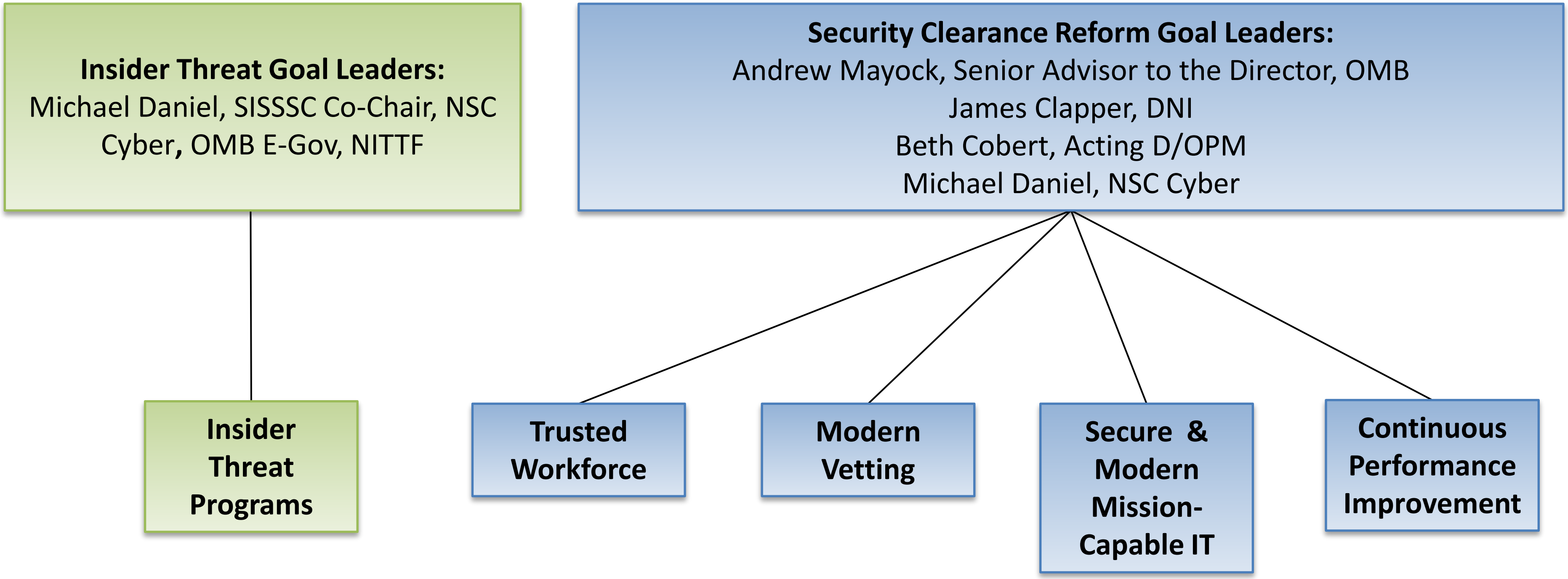
From April to June, in support of developing Insider Threat programs across government, the National Insider Threat Task Force:

- Trained 100 individuals from 40 agencies on Insider Threat hub operations
- Conducted independent assessments of five agencies to gauge community progress
- Co-hosted an Insider Threat Symposium with Carnegie Mellon University's Software Engineering Institute to share best practices
- Briefed Federal councils (e.g., CIO and HR) of insider threat program stakeholders to raise awareness

Action Plan Summary

Impact Area / Sub-Goal	Major Actions to Achieve Impact (See Page 18 for ITSCR Key Indicators)
Trusted Workforce	• Develop aligned and consistent policy for reporting potential security risks or observable behaviors of concern • Train and educate the Federal workforce on their vital role in the early detection of potential issues or risks • Build an SSC awareness campaign to reinforce the early identification of reportable behaviors • Study other related mission areas for potential information-sharing opportunities to streamline processes
Modern Vetting	• Establish an agile, data-driven and transparent policy making process which simplifies traditional overly complex policy development processes • Review current end-to-end SSC processes and identify the most cost-effective and efficient methods to vet the Federal workforce • Professionalize the SSC workforce through community training, certificate programs, and collaboration with universities
Secure and Modern Mission-Capable IT	• Modernize the SSC vetting lifecycle through the use of agency federated systems and shared services • Identify enhanced security and interoperability standards and capabilities to better inform IT cost and planning decisions • Provide agencies with a mechanism to adopt modern technology, automate manual processes, reduce duplicative investments, and decrease the cyber threat footprint
Continuous Performance Improvement	• Establish and implement outcome-based performance metrics and measures • Develop a Research and Innovation program to inform policy, process, and technology with empirical data-driven decisions • Establish a Continuous Performance Improvement model that will continuously evaluate the performance of the SSC policies and processes
Insider Threat Programs	• Assist departments and agencies in achieving program establishment, IOC and FOC by: providing training, technical advice and assistance; sharing best practices; issuing standards, direction and guidance; and advocating on behalf of insider threat programs • Conduct independent assessments to validate progress, and identify gaps and mitigations

CAP Goal Governance



Insider Threat Goal Leaders:
Michael Daniel, SISSSC Co-Chair, NSC Cyber**,** OMB E-Gov, NITTF

Security Clearance Reform Goal Leaders:
Andrew Mayock, Senior Advisor to the Director, OMB
James Clapper, DNI
Beth Cobert, Acting D/OPM
Michael Daniel, NSC Cyber

Insider Threat Programs

Trusted Workforce

Modern Vetting

Secure & Modern Mission-Capable IT

Continuous Performance Improvement

CAP Goal Governance – The PAC (OMB, ODNI, OPM, DoD, DHS, Treasury, DOJ, FBI, Energy, GSA, State, NARA and NSC) are responsible for driving government-wide implementation of these goals. In addition, the PAC PMO, EIB, and SSCLoB are enabling organizations responsible for tracking and monitoring goals and ensuring accountability.

Work Plan: Trusted Workforce

Problem being targeted: Information of security concern often goes unreported in the Federal government which inhibits an agency’s ability to address potential issues before escalation. This is mainly due to: a lack of government-wide reporting requirements; inconsistent training for supervisors and the overall Federal workforce; gaps in information sharing between the SSC community and related missions, such as human resources and insider threat; and inadequate communication on the importance of the Federal workforce and their vital role.

Theory of change: The SSC must work towards instilling a sense of shared responsibility by enabling a trusted workforce through consistent reporting requirements, employee and supervisor training, awareness campaigns for reportable behaviors, and identification of gaps in information sharing with sister missions.

Milestone Summary			
Key Milestones	**Milestone Due Date**	**Milestone Status**	**Owner**
Establish a policy that requires the national security population to report information of security concern to the proper authorities in a timely manner.	Dec-2016	On Track	ODNI
Identify overlaps and gaps in the data collected by the SSC community and other related mission areas, and recommend initiatives to align, integrate and improve information sharing.	Oct-2017	Not Started	ODNI, OPM, CredEA (TBD), PAC
Establish a policy that requires the entire Federal workforce (national security and non-national security) to report information of security concern to the proper authorities in a timely manner.	Apr-2019	Not Started	ODNI, OPM, CredEA (TBD)

Work Plan: Modern Vetting

Problem being targeted: The SSC community must keep pace with an ever changing global environment with an increasingly mobile workforce, emerging global threats, and advancements in cutting-edge technology and innovations. Comprehensive and impactful end-to-end reform has been limited due to: a lengthy policy-making process; manual and out-of-date vetting tools and methodologies; varying core suitability/fitness and credentialing adjudicative criteria and guidelines across the Federal government; and inconsistent implementation of aligned training standards.

Theory of change: To successfully modernize our vetting processes, the SSC community must develop agile vetting capabilities that integrate the latest innovative technologies to facilitate more continuous vetting of our trusted workforce and promote delivery of real-time information to the appropriate SSC professional responsible for making risk-based vetting decisions to protect the Federal government's personnel, property, and information systems.

Milestone Summary

Key Milestones	Milestone Due Date	Milestone Status	Owner
Develop plans to implement improved investigator and adjudicator training to better identify and act upon subject falsification of information.	Oct-2016	Complete	PAC PMO
Set standards for granting and suspending access to HSPD-12 compliant cards/badges.	Oct-2016	On Track	OPM
Establish the National Background Investigations Bureau (NBIB) to replace and assume the mission of OPM's Federal Investigative Services, and be responsible for providing effective, efficient, and secure background investigations for the Federal Government.	Oct-2016	On Track	PAC, OPM
Establish a Federal Background Investigations Liaison Office within the NBIB to oversee and resolve issues between Federal, State, and local law enforcement entities when collecting criminal history record information for Federal background investigations.	Oct-2016	On Track	NBIB
Modify standard security/suitability forms by updating questions related to mental health, reporting requirements, and Continuous Evaluation (CE).	Oct -2016	On Track	ODNI, OPM, OMB, PAC

Work Plan: Modern Vetting

Milestone Summary			
Key Milestones	**Milestone Due Date**	**Milestone Status**	**Owner**
Provide a recommendation to the PAC on whether conducting background investigations should be an inherently governmental function, and if not, whether it could be performed by a not-for-profit company.	Oct -2016	Complete	PAC
Advise the PAC on whether to develop an "access score" capability based on the level of sensitive information a subject has been granted access to; and subject personnel with high access scores to additional monitoring.	Oct-2016	Complete	OMB, DoD, NSC
Develop standard criteria and procedures to assist agencies in appropriately responding to falsification in all types of SSC adjudications.	Oct-2016	On Track	PAC PMO
Analyze the GAO report on security clearance process reform to determine action items and next steps.	Oct-2016	Complete	OMB
Issue adjudicative guidelines for national security positions.	Dec-2016	On Track	ODNI
Review and document the end-to-end SSC vetting process through business process re-engineering (BPR) and make recommendations on efficient and effective approaches.	Mar-2017	On Track	NBIB, DoD
Develop training and educational materials through the Federal Background Investigations Liaison Office to help state and local data providers understand their legal obligations and the importance of information sharing, along with available funding options to offset the cost of automation.	Jun-2017	On Track	NBIB
Implement a CE policy for the Executive Branch that regularly assesses trusted insiders who have been granted, or are eligible for, access to classified national security information.	Oct-2017	On Track	ODNI
Implement the 2012 Federal Investigative Standards across the Executive Branch to streamline the investigative process and increase adjudicators' ability to assess the Federal workforce.	Dec-2017	On Track	ISPs, OPM, ODNI, CredEA (TBD)

Work Plan: Modern Vetting

Milestone Summary			
Key Milestones	**Milestone Due Date**	**Milestone Status**	**Owner**
Establish a Credentialing Executive Agent with responsibility for policy and oversight of credentialing matters that parallels the authorities and responsibilities of the Security and Suitability Executive Agents.	Dec-2017	Not Started	PAC
Develop mechanisms to improve the quality and efficiency of the end-to-end SSC vetting process.	Oct-2018	On Track	ODNI, OPM, CredEA (TBD), NBIB, DoD
Evaluate and provide the PAC a recommendation for the expansion of Continuous Vetting across the entire federal workforce in order to regularly assess the eligibility of all trusted insiders.	Oct-2018	Not Started	OPM, CredEA (TBD)
Build upon existing national training standards to develop and implement a national training program that consists of a common set of professional and certification standards that will further develop and strengthen the SSC workforce.	Oct-2020	Not Started	ODNI, OPM, CredEA (TBD), DoD
Strengthen and align SSC adjudication standards so that relevant vetting information can be accessed and shared rapidly across the Executive Branch to support reciprocity.	Oct-2021	Not Started	ODNI, OPM, CredEA (TBD), PAC PMO, OMB

Work Plan: Secure & Modern Mission-Capable IT

Problem being targeted: The end-to-end SSC vetting process relies heavily on data sharing and information technology (IT) to operate efficiently, effectively, and securely. The SSC IT infrastructure has faced many challenges such as: aging system technology (both hardware and software) and legacy system architectural design; an IT environment that does not fully meet the needs of end users; and redundant stove-piped systems.

Theory of change: The SSC mission must develop and deploy a modern, secure, and mission capable end-to-end digital environment that builds on a foundation of government-wide standards, promotes interoperability and information sharing, and collaboration across the SSC community.

Milestone Summary

Key Milestones	**Milestone Due Date**	**Milestone Status**	**Owner**
Develop, build, and deploy a record repository to store unclassified SSC background investigation and adjudication history that can be shared across the SSC community.	Jan-2018	Not Started	NBIB, DoD
Streamline information-sharing agreements for use within the SSC community to allow for efficient data sharing and timely completion of SSC mission improvements.	Jul-2018	On Track	PAC PMO
Implement a CE system for the Executive Branch to continuously assess trusted insiders that are eligible for a national security position or access to classified information.	Sept-2018	On Track	ODNI
Develop and implement an Interagency Cybersecurity Response for SSC IT audits/reviews to further protect and secure SSC IT systems.	Oct-2018	Not Started	OPM, ODNI, CredEA (TBD)
Establish interoperability standards to maximize IT investments, and increase data collection and sharing across the SSC community.	Oct-2019	Not Started	PAC, EIB, SSCLoB
Provide the SSC community an efficient, cost-effective, and secure set of shared services to support the end-to-end SSC processes.	Oct-2020	On Track	ODNI, OPM, CredEA (TBD), DoD, NBIB

Work Plan: Continuous Performance Improvement

Problem being targeted: The SSC has faced challenges in monitoring performance and identifying and driving enterprise-level enhancements to policy, oversight, and operational processes. This is mainly due to the limited collection of enterprise-wide quality, effectiveness, and efficiency performance metrics; minimal feedback received when considering stakeholder equities and agency requirements; and the inability to fully leverage research and innovation within the SSC mission.

Theory of change: To initiate the necessary culture shift across the enterprise, the SSC community must institutionalize and integrate a continuous performance improvement model that will establish outcome- based performance metrics and measures, inform policy, process, and technology with empirical-based decisions, and continuously evaluate its performance and identify efficient and effective ways to perform its mission.

Milestone Summary

Key Milestones	**Milestone Due Date**	**Milestone Status**	**Owner**
Issue the PAC Strategic Intent and Enterprise IT Strategy Implementation Plan to synchronize reform efforts across the SSC community.	Oct-2016	On Track	PAC PMO, ODNI, OPM, DoD
Align the DOD modernization strategy for personnel security processes with the PAC Strategic Intent to ensure a national level effort in standardized processing and reinforcement of reciprocity.*	Oct-2016	Complete	DoD
Develop outcome-based metrics to measure the effectiveness of the DOD modernization strategy for personnel security processes to ensure alignment with the PAC Strategic Intent and Enterprise IT Strategy Implementation Plan.*	Oct-2016	Complete	DoD
Establish the PAC PMO, EIB, and SSCLoB as the Executive Branch organizations that will institutionalize end-to-end continuous performance improvement for the SSC mission.	May-2017	On Track	PAC, OMB
Develop and implement outcome-based metrics to measure the quality, efficiency and effectiveness of PAC reform efforts and the success of the SCC mission.	Oct-2017	On Track	PAC PMO

*The DoD modernization strategy is represented in the PAC Strategic Intent which provides overarching business direction for all agencies within the SSC mission space. This milestone has been completed in line with the PAC Strategic Intent.

Work Plan: Develop Insider Threat Programs

Alignment Goals:

- E.O. 13587, Steering Committee Priority #2: *Establish Insider Threat Programs*

Major Actions:

- Achieve program establishment
- Achieve Initial Operating Capability (IOC), see detailed IOC requirements on next slide
- Achieve Final Operating Capability (FOC), see detailed FOC requirements on next slide

Milestone Summary

Key Milestones	**Milestone Due Date**	**Milestone Status**	**Owner**
Achieve establishment criteria*	1/2015	Missed**	NITTF
Achieve IOC*	12/2015	Missed***	NITTF
Achieve FOC*	12/2016	At Risk****	NITTF

**Defined on next slide.*

***Most of the Executive branch D/As have accomplished program establishment tasks. Many D/As are discovering challenges with issues such as organizational culture, legal questions, and resource identification, to name a few. The NITTF is working to address these issues as quickly as possible.*

****Some Executive branch D/As have accomplished this task. However, many of those that have not are discovering challenges with issues such as organizational culture, legal questions, and resource identification, to name a few. The NITTF is working to address these issues as quickly as possible.*

*****Some Executive branch D/As have accomplished this task. The NITTF is assisting the remaining D/As in an effort to get them to FOC by the goal date.*

Work Plan: Develop Insider Threat Programs (cont.)

Requirements for Insider Threat Programs

Major Action #1: **Program Establishment** Basic requirements	*Major Action #2:* **Initial Operating Capability (IOC)** Program establishment plus the following	*Major Action #3:* **Final Operating Capability (FOC)** IOC plus the following
Name a responsible senior official(s)	Procedures in place for oversight, reporting, and record retention	Regular (if possible, electronic) access to insider threat-related indicators from counterintelligence, security, information assurance, HR, law enforcement, etc.
Promulgate an agency head-signed Insider Threat Program policy	Some capability to pull data from appropriate sources to retroactively analyze and respond to anomalies	Tailored indicators to monitor cleared user activity on any agency classified network accessed
Develop an Insider Threat Program implementation plan	Monitoring of user activity on at least one classified network	Access to counterintelligence reporting and adversarial threat information
	Employee notification of monitoring (i.e., banner)	A centralized "hub" to proactively assess data
	Annual employee awareness training	Response capability to follow-up on anomalous activity
	Trained Insider Threat Program personnel	Conduct self-assessments

ITSCR Key Indicator Portfolio

TW=Trusted Workforce MV = Modern Vetting IT = Secure & Modern Mission-Capable IT CPI = Continuous Performance Improvement

Metric ID	Key Indicator Title	Description	Projected Initial Collection Date	How Will It Be Used?
MV-1	End-to-End Process Timeliness for Investigations and Adjudications	Average number of days to complete end-to-end processing of investigations and adjudications for the national security population	Currently Collecting	Calculate enterprise timeliness metrics across key SSC business processes to determine areas of strength and potential weakness, and best practices
MV-2	National Security Population Eligibility and Access	Total number of Federal workforce eligible for a national security position and personnel currently in access	Mar-2017 Currently collecting for DoD	Measure efforts by agencies to decrease their national security population in line with SecEA policy
MV-3	Out-of-Scope National Security Population	Total number of Federal workforce eligible for a national security position with out-of-scope investigations	Mar-2017 Currently collecting for TS/SCI and DoD Secret populations	Measure efforts by agencies to prioritize their national security population and decrease overdue reinvestigations IAW SecEA policy
MV-4	Reciprocity	Total reciprocity actions, timeliness of reciprocal actions by agency	Mar-2017	Measure effectiveness of reciprocity across Executive branch and by agency
IT-1	Number of automated adjudications (eAdjudications) by case type	Total number of automated adjudications by case type	Mar-2017	Measure volume and cost savings of automated adjudications
MV-5	Number of Pending Investigations	Total number of pending investigations by investigation type and time category (by ISP)	Oct-2017	Measure volume of pending initial and periodic investigations to determine backlog scope
MV-6	2012 Federal Investigative Standards Compliance	Percentage of ISPs that are compliant with the revised investigative standards by tiers	Oct-2017	Evaluate efficiency and quality of modernizing the SSC investigative process

Key Indicators – MV1: End-to-End Process Timeliness

Average number of days to complete end-to-end processes at the 90th percentile by case type as defined under IRTPA.

Government-Wide Security Clearance Performance

(PAC Methodology)

Fastest 90%

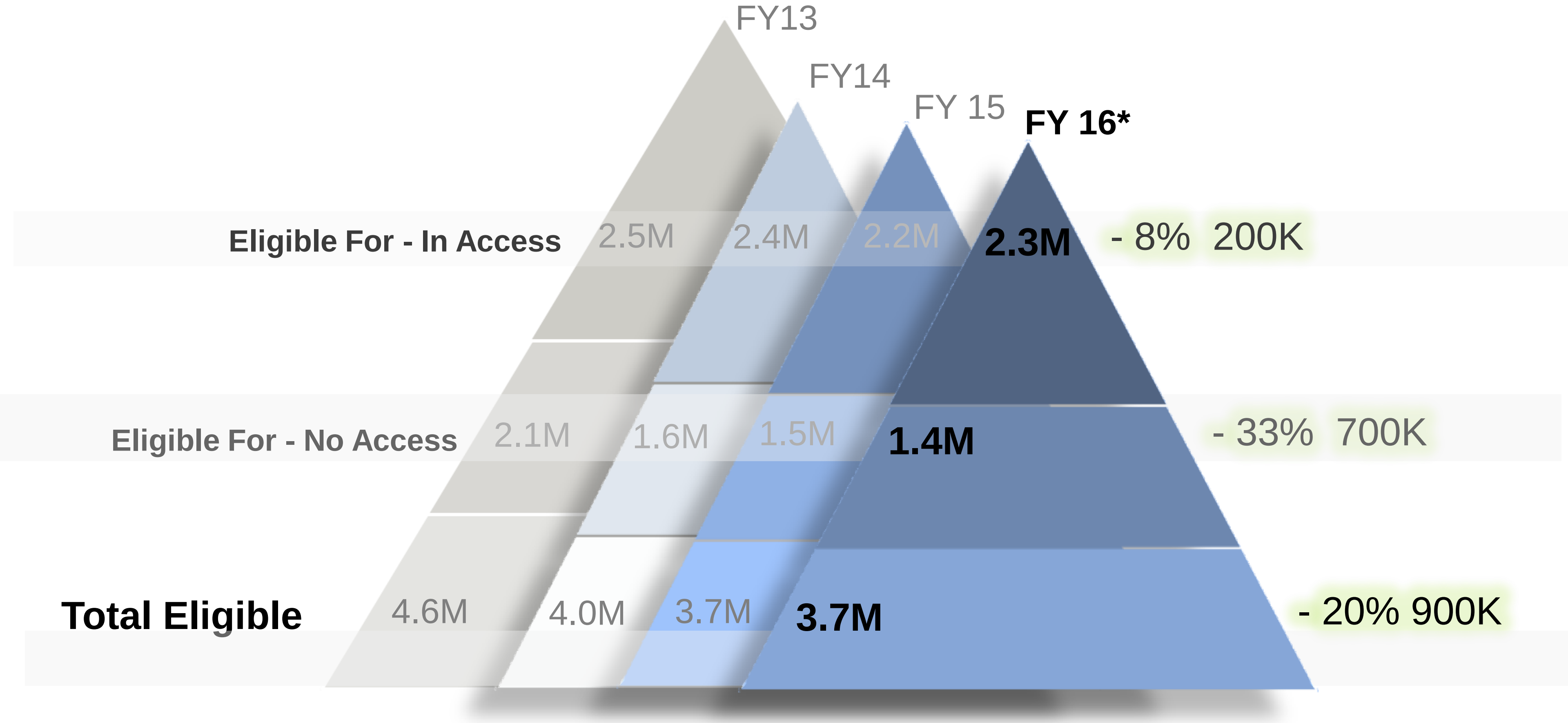
		Initiate				Investigate				Adjudicate				End-to-End (Initiate + Inv. + Adj.)			
		Average Days				Average Days				Average Days				Average Days			
		Q4 15	Q1 16	Q2 16	Q3 16	Q4 15	Q1 16	Q2 16	Q3 16	Q4 15	Q1 16	Q2 16	Q3 16	Q4 15	Q1 16	Q2 16	Q3 16
Initial Secret Cases	Volume	Goal: 14 Days				40 Days				20 Days				74 Days			
	343,557	9	9	9	9	66	92	128	123	20	9	15	15	95	116	152	147
Initial Top Secret Cases	Volume	Goal: 14 Days				80 Days				20 Days				114 Days			
	72,566	14	19	17	16	146	168	170	175	19	16	19	19	179	203	206	210
Periodic Reinvestigations	Volume	Goal: 15 Days				150 Days				30 Days				195 Days			
	156,172	12	12	12	12	211	192	175	177	28	23	22	22	237	227	209	211

Red Text: Goal Not Met

Blue Text: Goal Met

Key Indicators – MV2: DoD “In Access” and “Eligible” Populations*

Decrease in DoD Clearances from FY13 to FY16 (Cumulative)



Source: DoD Reporting to ODNI   * FY16 3rd Quarter Reporting

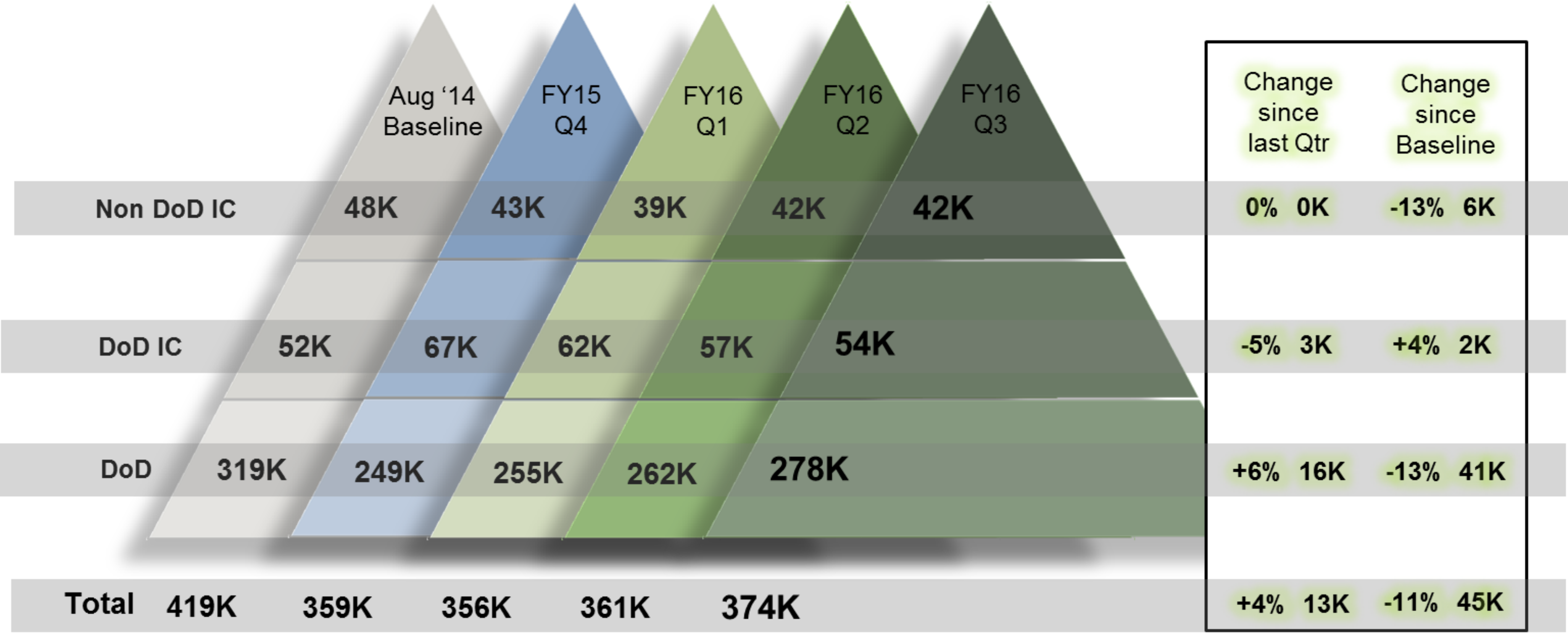
1 Jul 2016

**Responsive to the following Major Actions:*

- *Reduce period reinvestigation backlog using a risk-based approach*
- *Reduce total population of 5.1 M Secret and TS/SCI clearance holders to minimize risk of access to sensitive information and reduce costs*

Key Indicators – MV3: TS and TS/SCI “Out of Scope” Populations

TS and TS/SCI “Out of Scope” Populations



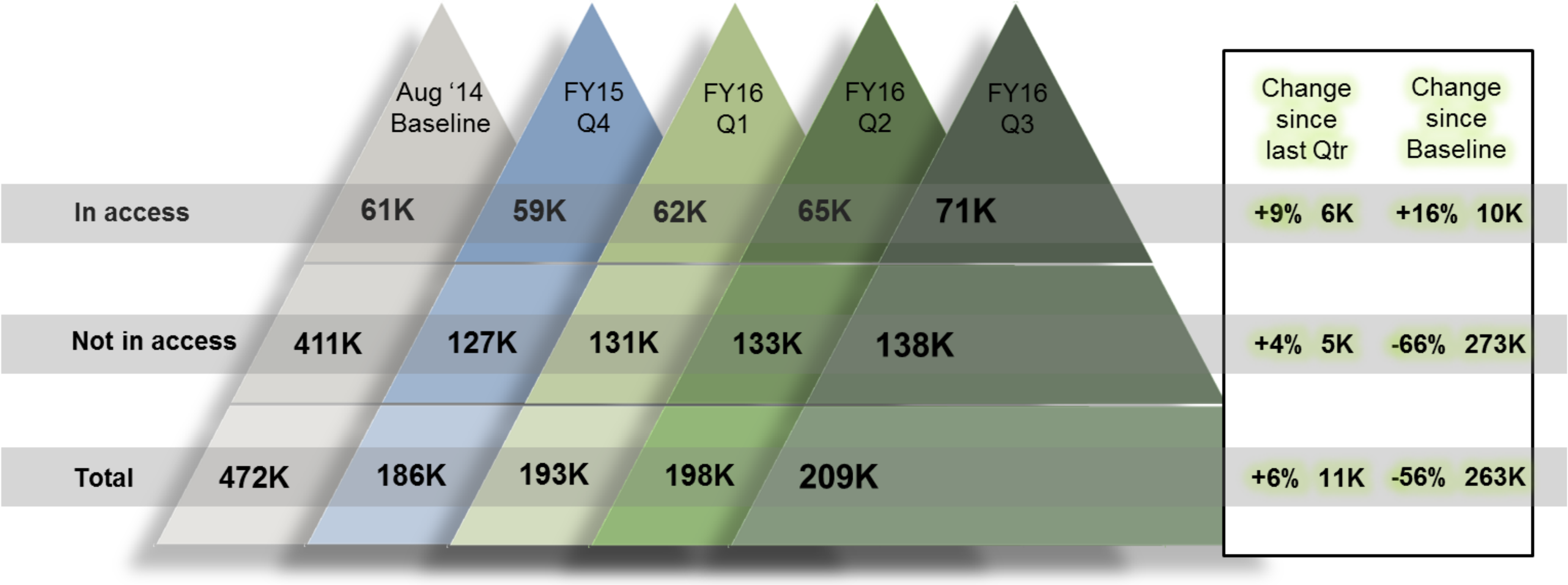
	Aug ‘14 Baseline	FY15 Q4	FY16 Q1	FY16 Q2	FY16 Q3	Change since last Qtr	Change since Baseline
Non DoD IC	48K	43K	39K	42K	42K	0% 0K	-13% 6K
DoD IC	52K	67K	62K	57K	54K	-5% 3K	+4% 2K
DoD	319K	249K	255K	262K	278K	+6% 16K	-13% 41K
Total	419K	359K	356K	361K	374K	+4% 13K	-11% 45K

Overall change since baseline: **-11% 45K**

7/1/2016 Source: Scattered Castles & JPAS

Key Indicators – MV3: DoD Secret “Out of Scope” Populations

DoD Secret “Out of Scope” Populations



	Aug ‘14 Baseline	FY15 Q4	FY16 Q1	FY16 Q2	FY16 Q3	Change since last Qtr	Change since Baseline
In access	61K	59K	62K	65K	71K	+9% 6K	+16% 10K
Not in access	411K	127K	131K	133K	138K	+4% 5K	-66% 273K
Total	472K	186K	193K	198K	209K	+6% 11K	-56% 263K

Overall change since baseline: -56% 263K

7/1/2016 Source: JPAS

Key Indicators – Insider Threat

Key Implementation Data

Sub-Goal	Indicator	Source	Baseline	Target	Frequency	Latest data	Trend
Insider Threat Programs	Percentage of agencies that have satisfied the program establishment criteria	NITTF Assessments*	0%	100%	As conducted	June 2016	
	Percentage of agencies that have achieved IOC	NITTF Assessments*	0%	100%	As conducted	June 2016	
	While in progress, the latest projected date for an agency achieving IOC	NITTF Assessments*	0%	100%	As conducted	June 2016	
	Percentage of agencies that have achieved FOC	NITTF Assessments*	0%	100%	As conducted	June 2016	
	While in progress, the latest projected date for an agency achieving FOC	NITTF Assessments*	0%	100%	As conducted	June 2016	

**Results of independent assessments conducted by the NITTF are classified and are not displayed in this report.*

Acronyms

- BI – Background Investigations
- CAP – Cross Agency Priority
- CE – Continuous Evaluation
- CFR – Code of Federal Regulations
- CIO – Chief Information Officer
- CPI – Continuous Performance Improvement
- CredEA – Credentialing Executive Agent
- CV – Continuous Vetting
- D/A – Department or Agency
- DDM – Deputy Director of Management
- DHS – Department of Homeland Security
- DNI – Director of National Intelligence
- DoD – Department of Defense
- DoE – Department of Energy
- DOJ – Department of Justice
- EA – Executive Agent
- EIB – Enterprise Investment Board
- EO – Executive Order
- eQIP – electronic Questionnaire for Investigations Processing
- FBI – Federal Bureau of Investigation
- FIS – Federal Investigative Standards
- FOC – Full Operating Capability
- FSO – Facility Security Officer
- FY – Fiscal Year
- GAO – United States Government Accountability Office
- GSA – General Services Administration
- HHS – Department of Health and Human Services
- HR – Human Resource
- IC – Intelligence Community
- IOC – Initial Operating Capability
- IRTPA – Intelligence Reform and Terrorism Prevention Act of 2004
- ISP –Internet Service Provider? (referenced as Executive Branch ISPs)
- IT – Information Technology
- ITSCR – Insider Threat and Security Clearance Reform
- KISSI – Key Information and Safeguarding Indicators
- LOB – Line of Business
- MV – Modern Vetting
- NARA – National Archives and Records Administration
- NBIB – National Background Investigative Bureau
- NITTF – National Insider Threat Task Force
- NLETS – National Law Enforcement Telecommunications System
- NSA – National Security Agency
- NSC – National Security Council
- ODNI – Office of the Director of National Intelligence
- OMB – Office of Management and Budget
- OPM – Office of Personnel Management
- PAC – Performance Accountability Council
- PAC AG – Performance Accountability Council Advisory Group
- PM/ISE – Program Manager/Information Sharing Environment
- PMA – President's Management Agenda
- PMO – Project Management Office
- PR – Periodic Reinvestigation
- QAS – Quality Assessment Standards
- SEAD – Security Executive Agent Directive
- SecEA – Security Executive Agent
- SISSSC – Senior Information Sharing and Safeguarding Steering Committee
- SSCLoB – Security, Suitability, and Credentialing Line of Business
- State – Department of State
- SuitEA – Suitability Executive Agent
- TBD – To Be Determined
- Treasury – Department of the Treasury
- TS/SCI – Top Secret/ Sensitive Compartmented Information
- TW – Trusted Workforce
- VA – Department of Veterans Affairs