Today, the Administration is announcing a series of changes to modernize and strengthen how the Federal Government performs and safeguards background investigations for its employees and contractors.

The Federal Government is responsible for issuing, handling and storing much of America’s most important data. The Government also performs key functions with these data, such as conducting background investigations to assess whether individuals may serve as Federal employees, members of the Armed Forces, or contractors, be granted access to its facilities and information systems, and be trusted with classified and other sensitive information. As the world’s technologies continue to evolve and our economy becomes ever more digitally connected, the Federal Government’s tools, systems, and processes for managing such sensitive information and conducting background investigations must keep pace with these advancements in order to better anticipate, detect, and counter malicious activities, as well as threats posed by trusted insiders who may seek to do harm to the Government’s personnel, property, and information systems.

Last year, in light of increasing cybersecurity threats, including the compromise of information housed at the Office of Personnel and Management (OPM), the Administration initiated a 90-Day Suitability and Security review to re-examine reforms to the Federal background investigations process, assess additional enhancements to further secure information networks and systems, and determine improvements that could be made to the way the Government conducts background investigations for suitability, security and credentialing. This review was conducted by the interagency Performance Accountability Council (PAC), which is chaired by the Office of Management and Budget (OMB) and comprised of the Director of National Intelligence (DNI), the Director of OPM, in their respective roles as Security and Suitability Executive Agents of the PAC, and the Departments of Defense (DOD), the Treasury, Homeland Security, State, Justice, Energy, the Federal Bureau of Investigation, and others. It also included consultation with outside experts.

The Administration is announcing today the results of that review, and steps we are taking to improve the Government’s security clearance and background investigation processes for Federal employees and contractors. These actions include establishing a new Federal entity, which will strengthen how the Federal Government performs background investigations. The actions will also assign the Department of Defense (DOD) responsibility for the IT security of and data related to the background investigations systems for the new entity. These actions will create a more secure and effective Federal background investigations infrastructure.
- **Establishing a New Federal Entity to Strengthen How the Government Performs Background Investigations.** OPM’s Federal Investigative Services (FIS) currently conducts investigations for over 100 Federal agencies – approximately 95 percent of the total background investigations government-wide – including more than 600,000 security clearance investigations and 400,000 suitability investigations each year. As part of the reforms being announced today, the Administration is establishing a new government-wide service provider for background investigations, the National Background Investigations Bureau (NBIB), which will assume this mission and absorb FIS. NBIB will concentrate solely on providing effective, efficient, and secure background investigations for the Federal Government. NBIB will report to the OPM Director, but unlike the previous structure, DOD will assume responsibility for the design, development, security, and operation of the background investigations IT systems for the new entity. Additional changes include: the head of NBIB will be Presidentially-appointed and a full member of the PAC; NBIB will receive policy direction and guidance from and be accountable to the PAC and its customer agencies for providing continuous improvements to the investigative process; NBIB will be headquartered in Washington D.C., which will allow for enhanced coordination with its interagency partners; and NBIB will have a dedicated senior privacy official to advance privacy-by-design as the new entity is stood up and new IT systems are developed. A cadre of interagency personnel will help stand up the new entity and be part of its ongoing management, and NBIB will leverage existing expertise, resources, and a well-established framework for providing government-wide services.

- **Leveraging Expertise at DOD for Processing Background Investigations and Protecting Against Threats.** To leverage the latest modern technology, protect the sensitive information used to effectively adjudicate investigations, and bring the fullest security resources to bear against increasingly sophisticated and evolving threats, NBIB’s information technology systems will be designed, built, secured, and operated by DOD, in accordance with NBIB requirements. This approach will leverage DOD’s significant national security, IT, and cybersecurity expertise, incorporating security into the fundamental design of the systems, strengthening the security of the data environment, and providing robust privacy protections. To support this work, the President’s Fiscal Year (FY) 2017 Budget will include $95 million in additional resources that will be dedicated to the development of these IT capabilities. The PAC will also establish an interagency cybersecurity advisory group to provide advice and counsel on system development and threat mitigation. These efforts are supported by the Federal Chief Information Officer’s call to Federal agencies to phase out the use of legacy IT systems, where possible, and begin
utilizing emerging technological tools and capabilities to adequately secure mission functions, systems, and information.

- **Updating Governance Authorities, Roles, and Responsibilities.** The current PAC and Executive Agent governance structure established by Executive Order 13467 will remain in place. However, the Administration will clarify existing roles within the enterprise and assign new responsibilities where gaps may exist by issuing new guidance as appropriate. For example, the Administration will establish a Credentialing Executive Agent with responsibility for policy and oversight of credentialing matters that parallels the respective authorities and responsibilities of the Security and Suitability Executive Agents. Currently, this responsibility is spread out across multiple agencies.

**Implementation**

While these changes will take time to fully implement, the Administration has taken and will continue to take immediate action to move forward with strengthening the background investigations process:

- **Build on the Security Measures Implemented in Response to the 2015 OPM Cyber Incidents.** In response to cybersecurity incidents at OPM last year, the Administration has taken a number of steps to strengthen the security of background investigation-related systems, including: expanding implementation of strong authentication for all users; increasing the number of scans for indicators of compromise; patching critical vulnerabilities; tightening policies and practices for privileged users; and identifying and prioritizing high value assets for additional security. OPM has also hired a new senior cyber and information technology advisor to support the ongoing response to these recent incidents, complete development of OPM’s plan to reduce the risk of future incidents, and recommend further improvements to secure OPM’s IT. These steps build on efforts the Administration has taken in recent months through the 30-day Cybersecurity Sprint and the release of the Cybersecurity Strategy Implementation Plan to increase our cybersecurity capabilities and protect systems and data government-wide.

- **Establish a NBIB Transition Team.** The Administration will establish a dedicated transition team headquartered in Washington D.C. to develop and implement a transition plan to: (1) stand-up the NBIB, (2) ensure that the transition timeline fully aligns with business needs, (3) transition the management of FIS IT systems to DoD, (4) migrate the existing mission, functions, personnel, and support structure of OPM
FIS to NBIB, and (5) provide continuity of service to customer agencies during the transition.

- **Drive Continuous Performance Improvement to Address Evolving Threats.** In order to ensure NBIB is successful in its critical mission, the PAC will: monitor performance in order to identify and drive enterprise-level process enhancements; make recommendations for changes to Executive Branch-wide guidance and authorities to resolve overlaps or close policy gaps where they may exist; and institute a data-driven, transparent policy-making processes. The PAC and the Performance Improvement Council will also develop, implement, and continuously re-evaluate and revise outcome-based metrics that measure the effectiveness of the vetting processes (e.g., security, investigative and adjudicative quality, cost, timeliness, reciprocity, customer service, and other performance characteristics).

Today’s announcement builds upon the Administration’s efforts to improve how the Government performs security clearance determinations, protecting the safety of American citizens and of our Nation’s most sensitive information and facilities.

These efforts include:

- Establishing a five-year reinvestigation requirement for all individuals with a security clearance, regardless of the level of access;  
- Reducing the number of individuals with active security clearances by 17 percent;  
- Launching programs to continuously evaluate personnel with security clearances to determine whether that individual continues to meet the requirements for eligibility; and,  
- Developing recommendations to enhance information sharing between State, local, and Federal Law Enforcement entities when conducting background investigations.

###