Memorandum on Integration, Sharing, and Use of National Security Threat Actor Information To Protect Americans

October 4, 2017

National Security Presidential Memorandum–7

Memorandum for the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of the Interior, the Secretary of Commerce, the Secretary of Energy, the Secretary of Homeland Security, the Assistant to the President and Chief of Staff, the Director of the Office of Management and Budget, the Assistant to the President and Senior Adviser, the Assistant to the President for National Security Affairs, the Counsel to the President, the Director of National Intelligence, the Assistant to the President for Science and Technology and Director of the Office of Science and Technology Policy, the Assistant to the President for Homeland Security and Counterterrorism, the Director of National Drug Control Policy, the Director of the National Counterterrorism Center, the Director of the Federal Bureau of Investigation, the Director of the Central Intelligence Agency, the Chairman of the Joint Chiefs of Staff, the Director of the National Security Agency, the Director of the Defense Intelligence Agency, the Co-Chairs of the President's Intelligence Advisory Board, the Administrator of Drug Enforcement, the Director of the National Geospatial Intelligence Agency, and the Archivist of the United States.

Subject: Integration, Sharing, and Use of National Security Threat Actor Information to Protect Americans

Section 1. Policy.

The United States Government's ability to effectively analyze, evaluate, integrate, correlate, and share classified national security information and other information concerning threat actors and their networks, and then use that information to support a broad array of national security missions and activities, is an essential component of our national security strategy. Equally important is the United States Government's ability to conduct these activities in a manner that: (a) appropriately protects the security and integrity of that information and its origins; (b) properly considers, approves, and monitors the information's application and use, consistent with applicable law and Presidential guidance; (c) ensures relevant operational deconfliction and security; and (d) maintains and uses the information in a manner that appropriately protects individuals' privacy, civil rights, and civil liberties, including by providing appropriate redress. Our continuing efforts to achieve these goals requires both systematic collaboration across national security components and integrated practices that fully utilize our collective data holdings to support vital national security missions.

Therefore, to protect against actors who threaten our Nation, it is the policy of the United States to: (a) lawfully identify, integrate, and make available thorough, accurate, and timely national security threat actor information; (b) effectively manage that information within appropriate policy frameworks and technical architectures, including data repositories, integrated systems, and cloud architectures; (c) where appropriate and consistent with applicable law, deliberately use that information to support national security activities; and (d) where appropriate and consistent with applicable law, share relevant and releasable information, products, and outputs with foreign governments, international organizations, and State, local, territorial, tribal, and private-sector partners where required to support activities

that benefit national security. National security threat actor information comprises identity attributes and associated information about individuals, organizations, groups, or networks assessed to be a threat to the safety, security, or national interests of the United States that fall into one or more of the categories listed in the annex to this memorandum.

This memorandum shall be implemented in a manner that is consistent with applicable law and Presidential guidance; safeguards intelligence sources, methods, and activities; protects otherwise sensitive information and preserves the integrity of sensitive operations and investigations; and appropriately protects privacy, civil rights, civil liberties, and other constitutional and statutory rights, including through compliance with applicable guidelines governing the collection, retention, and dissemination of personally identifiable information.

Sec. 2. Definitions.

The following definitions shall apply throughout this memorandum:

Associated information: Information that demonstrates the meaningful (i.e., non-incidental) associations, capabilities, intentions, and activities of an individual, organization, group, or network.

Identity attributes: Information (including biometric and biographic data) that can be used independently or in combination with other data to identify a specific individual.

Sec. 3. Implementation.

To strengthen the ability of the United States Government to protect against individuals who threaten our national security interests or the safety of United States citizens, and consistent with applicable law and the policy set forth in section 1 of this memorandum:

A. The Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall lead, in consultation and coordination with the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Secretary of Energy, and the Director of the Central Intelligence Agency, the development and implementation of appropriate technical architectures and corresponding policy frameworks to advance the integration, sharing, and use of identity attributes and associated derogatory information for each individual category of evaluated national security threat actor information described in the annex to this memorandum. The technical architecture and corresponding policy framework for each category shall be developed in a manner that appropriately protects the security and integrity of information; enables the appropriate analysis, sharing, and use of information to the extent permitted by and consistent with applicable law; ensures relevant operational deconfliction and security; and provides for the maintenance and use of such information in a manner that appropriately protects individuals' privacy, civil rights, civil liberties, and other constitutional and statutory rights, including through compliance with applicable guidelines governing the collection, retention, and dissemination of personally identifiable information.

B. Through the development, implementation, and ongoing execution of each technical architecture's policy framework, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, in coordination with the Secretary of State, the Secretary of the Treasury, the Secretary of Energy, and the Director of the Central Intelligence Agency, shall regularly assess both the technical architectures and the current or proposed applications and uses of the

evaluated national security threat actor information they manage to determine if the architectures or any of their specific applications or uses should be enhanced, modified, or terminated. These assessments shall consider the potential risks and benefits to national security, legal or policy concerns, and the resource implications of enhancing, modifying, or terminating any aspect of the technical architectures or their applications and uses. Further, these assessments shall define the appropriate access protocols, data standards, security safeguards, and operational deconfliction mechanisms required to meet legal, policy, or mission requirements. These assessments shall be a continuing responsibility for the heads of the executive departments and agencies (agencies) identified in this subsection.

C. The Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, in consultation with the Secretary of State, the Secretary of the Treasury, and the Secretary of Energy, shall jointly identify, as between themselves, the department or agency (or component thereof) best suited to serve as the executive agent for each individual category of national security threat actor information. The executive agent shall be responsible for developing and maintaining that category's specific technical architecture, its corresponding policy framework, and an appropriate governance mechanism to facilitate the capability reviews described in subsection (B) of this section.

D. Within the parameters defined by the appropriate policy frameworks developed under subsection (A) of this section, the heads of all agencies shall, to the maximum extent permitted by law and the greatest extent practicable in light of the need to protect sources and methods, sensitive information, and the integrity of ongoing operations and investigations, maintain and make available evaluated national security threat actor information within the relevant technical architectures.

E. For all applications and uses of national security threat actor information managed within the technical architectures established under subsection (A) of this section that seek or would be reasonably likely to result in the denial of a benefit or protected interest, the heads of the agencies responsible for such applications or uses shall first ensure that appropriate and lawful procedures and safeguards exist to protect individuals' privacy, civil rights, civil liberties, and other constitutional and statutory rights, and provide appropriate protections before the application or use goes into effect.

F. The Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology and in coordination with the Director of National Intelligence, shall, as part of its ongoing coordination of the development, publication, and evolution of national standards, lead a standing interagency effort, which shall include relevant elements of the Intelligence Community, to establish specific models for information exchange and corresponding application profiles for identity attributes relevant to the implementation of this memorandum. These national standards shall, to the extent practicable, be consistent with relevant voluntary international standards when such standards advance national security interests.

G. The heads of the agencies shall, to the extent practicable, implement the standards, formats, and application profiles developed pursuant to subsection (F) of this section within their system acquisition and research and development activities.

H. The Director of National Intelligence shall work with Intelligence Community elements to explore and implement solutions for standardizing and publishing key identity attributes captured within intelligence information reports in machine readable formats to support automated processing within the technical architectures established under subsection (A) of this section, in accordance with approved standards, formats, and application profiles established under subsection (F) of this section.

I. The Director of the Office of Science and Technology Policy, in coordination with the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, and the heads of other appropriate agencies, shall, through the National Science and Technology Council, work with departments and agencies to align and synchronize Federally-funded research and development activities that seek to enhance the integration, management, and use of national security threat actor information.

J. The Deputies Committee of the National Security Council may supplement, modify, or remove the categories of national security threat actors established pursuant to this memorandum. Upon approval by the Deputies Committee, changes to these categories shall be formally documented by updating the annex to this memorandum.

K. Within 270 days of the date of this memorandum, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, in coordination with the Secretary of State, the Secretary of the Treasury, and the Secretary of Energy, shall, through the Assistant to the President for Homeland Security and Counterterrorism, submit to the President a plan to implement this memorandum.

L. The Assistant to the President for Homeland Security and Counterterrorism shall, consistent with National Security Presidential Memorandum–4 of April 4, 2017, or any successor document, coordinate, facilitate, review, and, as appropriate, make recommendations concerning all policy aspects regarding the integration, sharing, and application and use of national security threat actor information and its implementation.

Sec. 4. General Provisions.

This memorandum does not alter existing statutory and regulatory authorities or responsibilities of agency heads to carry out operational activities or provide and receive information.

This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP

NOTE: The memorandum was released by the Office of the Press Secretary on October 5.

Categories: Communications to Federal Agencies : National security threat actor information, integration, sharing, and use, strengthening efforts, memorandum.

Subjects: Defense and national security : Classified national security information; Defense and national security : Intelligence.

DCPD Number: DCPD201700722.