Fact Sheet - DoD Manual 5240.01

The Department of Defense (DoD) has released an update to DoD Manual 5240.01. Executive Order 12333, United States Intelligence Activities, governs how agencies within the Intelligence Community conduct activities in support of their missions while safeguarding the legal rights and protections guaranteed to all U.S. persons by the Constitution and laws of the United States. DoD Manual 5240.01 implements the requirement in Executive Order 12333 that Intelligence Community elements establish procedures, approved by the Attorney General, after consultation with the Director of National Intelligence, governing the collection, retention, and dissemination of information concerning U.S. persons.

This version of the DoD Manual 5240.01 has been updated to align authorities and safeguards with the critical capabilities necessary for the Department to protect America's national security interests as well as individual rights and freedoms. The manual was last issued in 1982. In the intervening decades, there have been significant changes in technology, law, and intelligence practices: The information technology revolution has significantly affected intelligence collection and analysis capabilities and raised new issues regarding privacy and civil liberties. New and varied types of asymmetric threats have emerged, including threats from non-state terrorist actors, which have changed the way we defend our nation. Additional requirements have been imposed on the intelligence community, including new mandates for information sharing. And finally, new and significant roles and responsibilities have been defined within the intelligence community, including the establishment of the Director of National Intelligence, privacy and civil liberties officials, and intelligence oversight officials.

The new manual addresses these changes, while allowing for flexibility given the broad intelligence collection activities conducted across the Department of Defense enterprise.

The Classified Annex to Department of Defense Procedures, United States Signal Intelligence Directive (USSID) SP0018, "Legal Compliance and U.S. Persons Minimization Procedures," (January 25, 2011), and Presidential Policy Directive (PPD) 28 remain in effect.

What are the major changes?

Major changes to the manual include updated definitions for "collection" and "publicly available information" and new rules for DoD intelligence components regarding retention of U.S. person information (USPI); hosting or participating in shared data repositories; and conducting physical searches.

- Definition of "collection": One of the key changes to the manual is how we define "collection." "Collection" is defined in the revised procedures as occurring "upon receipt," which differs from the previous version of the manual, which defined "collection" as occurring when the information was "officially accept[ed] … for use." This is an important clarification that ensures that all of the protections in the guidelines, including protections governing the retention of USPI, apply to information upon receipt. This framework establishes better accountability of the information maintained by DoD and is consistent with how agencies define collection for all federal records. Because

information is deemed collected upon receipt, while information must be promptly evaluated, the retention periods that could apply to unevaluated information are longer than the 90-day period that applied under the previous guidelines, where information could be held for a longer period until it was affirmatively evaluated for use by DoD. As discussed below, the retention periods specifically account for different types of collection activities.

- New rules governing the protection and evaluation of information for permanent retention: The procedures now establish maximum evaluation periods that are based on how information is collected. The procedures require that, at the end of the maximum evaluation period, USPI and information that may incidentally include USPI is deleted from intelligence databases unless affirmatively determined to meet the criteria for permanent retention. The procedures include other enhanced safeguards and protections that apply during the evaluation period. These include access rules and query rules beyond those included in the old procedures.

- Special collection: To address those collections where privacy and civil liberties interests may be heightened, the manual now includes a new collection category of "special circumstances" collections. Special circumstances collections require consideration of additional handling safeguards based on the volume, proportion, and sensitivity of the USPI, and the intrusiveness of the collection method. These new “special circumstances” rules require an accountable senior intelligence official to make specific decisions about the intelligence value of the collection. The new rules also enhance the protection of USPI as the manual requires new considerations and protections if special circumstances exist.

- Shared repositories: The manual creates new rules for shared data repositories when a DoD intelligence component is the host of or a participant in a shared repository, and it provides guidance for dissemination of USPI within and outside the DoD to meet intelligence community information sharing requirements. These provisions reflect post-9/11 policy recommendations and Executive Branch policy decisions to enhance the sharing of information across the intelligence community.

- Publicly available information: Obtaining publicly available information is one of the least intrusive collection methods available to DoD intelligence components. The manual clarifies the definition of “publicly available” and adds context to several of its provisions by providing a more detailed characterization of what “publicly available” means, recognizing the policy issues raised by the Internet and new technology.

- New physical search rules: The manual also incorporates new rules regarding physical searches to reflect changes to the Foreign Intelligence Surveillance Act since 1982, including the requirement to obtain a FISA warrant for nonconsensual physical searches within the United States and for targeted collection of U.S. person information outside the United States.

How long may DoD retain US Person Information?

The revised procedures make clear that collected information must be promptly evaluated and establish how long DoD can retain USPI for evaluation to assess whether the information meets the permanent retention standard. The fundamental privacy principle embodied in the procedures is that information will be deleted at the end of the appropriate maximum retention period unless it is affirmatively determined to meet the standard for permanent retention. These evaluation periods differ depending on the nature of the collection and the nature of the information collected. For intentionally collected USPI, those records may, if necessary, only be retained for evaluation for up to 5 years. Incidentally collected USPI may be retained for evaluation for up to 5 years if the collection targeted a person or place in the United States or involves "special circumstances," and up to 25 years if the collection targeted a person who is reasonably believed to be outside the United States. All USPI, including any information that may contain USPI, must be deleted upon expiration of these evaluation periods unless it has been determined to meet the standard for permanent retention. These periods can only be extended based on high-level approval, which requires a written finding of necessity and a finding that the information is likely to contain valuable information.

These evaluation periods were developed in collaboration with intelligence analysts, technologists, policy makers, legal counsels, and privacy and civil liberties and intelligence oversight officials. Data is an important asset to the intelligence community. In developing these evaluation periods, the objective throughout was to consider the practical utility of retaining data for evaluation to maximize the effectiveness of the intelligence mission while respecting and incorporating principles that protect the privacy and civil liberties of U.S. persons.

What are the privacy protections and oversight requirements?

Privacy protections and oversight requirements include:

- Changes to the definition of "collection," which applies all of the safeguards and requirements to USPI when "received" rather than when "officially accept[ed] … for use;"
- Recognition of the importance of protecting the privacy and civil liberties of the American people;
- Express prohibition of the collection or maintenance of information about U.S. persons solely for the purpose of monitoring activities protected by the First Amendment and the Constitution;
- Express requirement on the Department to obtain USPI by the least intrusive method;
- Express limitation of the collection of non-publicly available USPI to no more than reasonably necessary for the mission;
- Establishment of rules for evaluating retention at the most specific level of information practicable;
- Establishment of new rules for dissemination, including requirements for disseminating unevaluated information, minimization of information disseminated, and explicit rules and analysis required for disseminating to foreign governments; and

- Establishment of additional oversight responsibilities for component heads, privacy and civil liberties officials, intelligence oversight officials, and offices of the general counsel.

What was the process for updating the procedures?

The process for updating the procedures was established to ensure that a diversity of views were considered and discussed and that the procedures could be implemented and followed by intelligence professionals tasked with executing the wide range of intelligence missions for which DoD is responsible. The update was overseen by the DoD Senior Intelligence Oversight Official, in coordination with officials from each of the Defense Intelligence Components, the Department of Justice (DOJ), and the Office of the Director of National Intelligence (ODNI). These officials included the Privacy and Civil Liberties Officer at DOJ, the Civil Liberties Officer at the ODNI, and the Senior Agency Official for Privacy of DoD.

In accordance with Executive Order 12333, the Secretary of Defense and the Attorney General approve the manual, after consultation with the Director of National Intelligence.