# *Procedure 3*
# *Retention of*
# *U.S. Person Information (USPI)*

# Agenda

- **Procedure 3 Applicability**
- **Key Changes**
- **A Practitioner's Summary with Key Takeaways**
- **ROE: Participate and Ask Questions**

# Procedure 3 Applicability

- ✓ **NEW:** Governs retention of USPI collected by Defense Intelligence Components (DICs) or disseminated by another Component or Intelligence Community (IC) element (Change from "govern[ing] .. information about [US] persons that may be knowingly retained…without consent"), para. 3.3.a
- ✓ **NEW:** Memorializes requirement for retention of USPI from SIGINT to follow the Classified Annex, para. 3.3.i
- ✓ Requires Maintenance and Disposition of USPI to conform with the DoD Component records management schedules, para. 3.3.h

- X Does not apply to retention of information obtained under the Foreign Intelligence and Surveillance Act, as amended, para. 3.3.a
- X Does not apply USPI obtained for an excluded mission under Procedure 1, para. 3.1.a(3)

**PRACTITIONER'S TIP 1:**
DoD's adoption of the new definition of "collection" elevates the need for you to understand US person information (USPI) retention rules, which are now far more complex & align with the IC.

# Procedure 3 – Key Changes

## DoDM 5240.01

- 3.3.a Scope
- 3.3.b Definition of Terms
- 3.3.c Evaluation of Information
  - (1) Intentional Collection of USPI
  - (2) Incidental Collection of USPI
  - (3) Voluntarily Provided USPI
  - (4) Special Circumstances
  - (5) Extended Retention
  - (6) Unintelligible Information
  - (7) Deletion of Information
- 3.3.d Information Disseminated by Another Component or [IC] Element
- 3.3.e Permanent Retention
- 3.3.f Protections for USPI
- 3.3.g Enhanced Safeguards
- 3.3.h Maintenance and Disposition of Information
- 3.3.i Signals Intelligence (SIGINT)

## DoD 5240.1-R

- C3.1 Applicability
- C3.2 Explanation of Undefined Terms
- C3.3 Criteria for Retention
  1. Retention of Information Collected Under Proc. 2
  2. Retention of Information Acquired Incidentally
  3. Retention of Information Relating to Functions of Other DoD Components or non-DoD Agencies
  4. Temporary Retention
  5. Retention of Other Information
- C3.4 Access and Retention
  1. Controls on Access to Retained Information
  2. Duration of Retention
  3. Information Acquired Prior to Effective Date

# Procedure 3 – Key Changes

## Key Terms

- **Retention (NEW)**
  - Maintenance of information, **either hard copy or electronic format**, **regardless of how collected or disseminated to a DIC**
- **USPI (NEW)**
  - Either a single item of information or when combined with other information, is reasonably likely to identify one or more specific U.S. persons.
  - May require a case-by-case assessment by a trained intelligence professional
  - NOT USPI
    - Reference to a product by brand or manufacturer's name
    - Imagery from overhead reconnaissance or Information about conveyances without linkage to additional identifying information that ties the information to a specific U.S. person
- **Reasonable Belief (Updated)**
  - Based on articulable facts and circumstances
- **Intentional Collection of USPI (NEW)**
  - Information deliberately sought by a DIC
- **Incidental Collection of USPI (NEW)**
  - Information not deliberately sought, nonetheless collected
  - Whether it is expected or reasonably anticipated to occur
- **Unintelligible Information (NEW)**
  - Undefined but with some clarification
  - "Includes information that a Component cannot decrypt or understand in the original format"
- **Others worth mentioning**
  - Special Circumstances Collection **(NEW)** - undefined
  - Defense Intelligent Component
  - Defense Intelligence Component Employee
  - "Prompt Evaluation" - undefined

PRACTITIONER'S TIP 2:
Before reviewing the USPI retention rules, ask yourself whether the activity being contemplated is within the scope of this Procedure by assessing key definitions particular to the retention analysis.

# Key Changes

## Basic Retention Rule

**DICs will evaluate information that may contain USPI to determine whether it may be permanently retained. (para. 3.3.e)**

- Two part Standard for Permanent Retention (if not for Oversight):
  - Reasonable belief retention of the USPI is necessary to perform an intelligence mission or function AND
  - One of the following:
    - Information was lawfully collected or disseminated, and meets a para. 3.2.c collection category; or
    - Information is necessary to understand or assess FI or CI
- Retention decision is made at the most specific level of information appropriate and practicable, para. 3.3.e.(3)

PRACTITIONER'S TIP 3:
Once you assess that the rules for retention are indeed applicable, the goal is to reach a conclusion on whether the information may be maintained permanently.

# Key Changes

## NEW Temporary Retention Rules

- **Standards for Temporary Retention Are Based on the Collection Type and location of the intended collection (para. 3.3.c)**
  - New temporary retention periods replace the 90-day retention period
  - Retention periods depend on location of the intended collection and type of collection:
    - Intentional Collection of USPI
    - Incidental Collection of USPI
    - Voluntarily Provided
    - Special Circumstances

**PRACTITIONER'S TIP 4:**
Sometimes you cannot evaluate USPI for permanent retention right away. You may temporarily retain USPI that falls within 1 of these 4 broad collection types. The retention type will guide you to the right retention rules and, more importantly, the temporary retention period.

# Key Changes

## NEW Temporary Retention Rules

### Types of Collection

**Intentional Collection of USPI**

- Requires prompt evaluation
- 5 years to evaluate
- Possible 5 year extension (Single Delegee)

**Incidental Collection of USPI**

- Focus is a person reasonably believed to be inside the US, 5 years to evaluate; Possible 5 year extension (Single Delegee)
- Focus was a person reasonably believed to be outside the US, 25 years to evaluate

**Voluntarily Provided USPI**

- Requires prompt evaluation
- 5 years to evaluate; Possible 5 year extension (Single Delegee)
- Focus is a Non-US person but may contain USPI, 25 years to evaluate

**Special Circumstances Collection**

- 5 years to evaluate
- If involves intentional collection of USPI, requires prompt evaluation and 5 years to evaluate
- Extension by USDI
- Enhanced Safeguards

PRACTITIONER'S TIP 5:
There are 4 broad collection types. Each collection type has specific retention periods, some of which permit extensions. Consult the table provided on the next slide for more information.

# Key Changes

## Standards for Retention

| Paragraph | Description | Example | Evaluation Period | Extension* |
|---|---|---|---|---|
| 3.3.c.(1) | **Intentionally collected USPI** Focus of the collection is a US person located inside or outside the US | Travel itinerary and foreign hotel bills with credit card information of a specific New York citizen who has traveled to Iraq to join an international terrorist organization | ***Promptly,*** or up to 5 years if necessary | • 5 years<br>• Approved by head of DIC or delegee<br>• May be given at time of collection or later |
| 3.3.c.(2)(a) | **USPI incidentally collected where target is in the US** Focus of the collection is non-US person located inside the US, and USPI is incidentally acquired | Travel VISAs for John E. Smith, a foreign national currently residing in New Jersey, which returned prior VISA's for Jon E. Smith, a lawful permanent resident of New York | 5 years | • Same as above |
| 3.3.c.(2)(b) | **USPI incidentally collected where target is outside the US -** Focus of the collection is a US or a non-US person overseas, and USPI is incidentally acquired | Imagery of the "Fair Winds", a yacht known to belong to a foreign narcotics smuggler anchored next to the "Blue Skies", a yacht belonging to a Florida citizen off the cost of the Bahamas. | 25 years | • No extension |
| 3.3.c.(3) | **Voluntarily provided USPI** Volunteered Information reasonably believed to be about a US Person | Thumb drive dropped off at the U.S. Embassy in France with a note on it that says "past 2 years of recruiting rosters for international terrorist outpost in California" | ***Promptly***, if necessary up to 5 years | • 5 years<br>• Approved by agency head or delegee<br>• May be given at time of collection or later |
| 3.3.c.(4) | **Special circumstances** | Thumb drive dropped off at the U.S. Embassy in France with a note on it that says "all patient files at a US hospital treating a key foreign target" | 5 years | • 5 years<br>• Approved by USD(I)<br>• May be given at time of collection or later |
| 3.3.d | **Information disseminated by another Component or IC element** | IC Element hosts a database of all known international terrorist groups | Same time as originating entity | • No extension |

# Key Changes

## NEW Extended Retention of USPI

- **May be approved by head of DIC, delegee, or USD(I) at time of collection or after for no more than 5 years**
- **Determination by the Approval Official Required**
  1. All of the following:
     - Retention is necessary to carry out an authorized Component mission
     - Retention and handling is consistent with protection of privacy and civil liberties
     - Must consider need for enhanced protections
     - Consultation with Component privacy and civil liberties official
  2. Information is likely to contain valuable information that the Component is authorized to collect in accordance with Procedure 2
- **Document Compliance**
- **Further extension accomplished through "exception to policy"**

PRACTITIONER'S TIP 6:
Extensions to the temporary retention periods are not automatic. Be sure to check your organization's Table of Delegations, and ensure extension criteria is met and documented.

# Key Changes

## NEW Deletion of USPI, para. 3.3.c.(7)

- **DICs must delete all USPI from the DIC's automated systems of records when:**
  - **DIC determines that the Standard for Permanent Retention has not been met , or**
  - **DIC cannot make a determination concerning the Standard for Permanent Retention in the specified temporary evaluation period (see chart for the periods)**

- **If Deletion is required, you also must delete any information that *may* contain USPI in the data set**

# Key Changes

## NEW Information Disseminated by Another Component or IC Element, para. 3.3.d

- Applies to information outside the collection definition because it was disseminated by another Component or IC element (per para. 3.3.a)
- Unevaluated Information
  - Unevaluated Information *that may contain USPI*
  - Only permitted to retain and evaluate it for permanent retention under para. 3.3.e for as long as the originating agency may retain it. (No authority to extend - you must call originator)
- Evaluated Information
  - Information already permanently retained by another Component or IC element
  - Only need to verify that the information is reasonably believed to be necessary for the performance of the recipient's authorized intelligence mission to permanently retain

**PRACTITIONER'S TIP 7:**
Data is an IC Asset. Because data is collected "upon receipt," it is in effect collected only once. Once collected, it is either unevaluated or evaluated. Apply the original collector's retention period for unevaluated data. For evaluated data (meaning data already approved for permanent retention), ask yourself if the information is reasonably believed to be necessary to perform your mission.

# Key Changes

## NEW Enhanced Safeguards

- **Applies to Special Circumstances Collection**
- **Step 1 - Determine Need for Enhanced Safeguards**
  - Intrusiveness of methods used to acquire USPI
  - Potential for substantial harm, embarrassment, inconvenience, or unfairness if USPI is improperly used or disclosed
  - Expected USPI use and expected searches or queries
  - Retention length & technical difficulties
  - Legal or policy restrictions or factors directed by USD(I)
- **Step 2 - Consider and Identify Measures**
  - Procedures for review, approval, auditing access or searches
  - Procedures to restrict access/dissemination
  - Use of privacy-enhancing techniques
  - Access controls
  - Additional training and protective retention measures

PRACTITIONER'S TIP 8:
For Special Circumstances Collection, the Head of DIC or delegee must follow a 2-part process. First, determine the need for enhanced safeguards and, then identify and implement appropriate. measures.

# Key Changes

## NEW Procedures to Protect USPI

- **Measures: DIC are responsible to protect USPI:**
  - Limit access to appropriate employees
  - Conduct relevant and tailored queries
  - Establish written query procedures
  - Audit information systems containing USPI
  - Document procedures for USPI data retention
  - Annual training for employees who access USPI
- **Marking: Identify & mark/tag files believed or known to contain USPI whether electronic or hard copy**
- **Review: periodically to practices and adequacy of retention periods**

PRACTITIONER'S TIP 9:
USPI protections require collaboration between the intelligence professionals who handle USPI, the IT professionals who make it accessible, the legal professionals who advise, the privacy and oversight officials who help enforce the provisions, and the head of Component who's ultimately responsible for compliance. These items are auditable and should be integrated in your oversight program.

# Practitioner's Summary

**PRACTITIONER'S TIP 1: (SLIDE 3)**
DoD's adoption of the new definition of "collection" elevates the need for you to understand US person information (USPI) retention rules, which are now far more complex & align with the IC.

**PRACTITIONER'S TIP 2: (SLIDE 5)**
Before reviewing the USPI retention rules, ask yourself whether the activity being contemplated is within the scope of this Procedure by assessing key definitions particular to the retention analysis.

**PRACTITIONER'S TIP 3: (SLIDE 6)**
Once you assess that the rules for retention are indeed applicable, the goal is to reach a conclusion on whether the information may be maintained permanently.

# Practitioner's Summary

**PRACTITIONER'S TIP 4: (SLIDE 7)**
Sometimes you cannot evaluate USPI for permanent retention right away. You may temporarily retain USPI that falls within 1 of 4 broad collection types. The retention type will guide you to the right retention rules and, more importantly, the temporary retention *period*.

**PRACTITIONER'S TIP 5: (SLIDE 8)**
There are 4 broad collection types. Each collection type has specific retention periods, some of which permit extensions. Consult the table provided for more information.

**PRACTITIONER'S TIP 6: (SLIDE 10)**
Extensions to the temporary retention periods are not automatic. Be sure to check your organization's Table of Delegations, and ensure extension criteria is met and documented.

# Practitioner's Summary

**PRACTITIONER'S TIP 7: (SLIDE 11)**
Data is an IC Asset. Because data is collected "upon receipt," it is in effect collected only once. Once collected, it is either unevaluated or evaluated. Apply the original collector's retention period for unevaluated data. For evaluated data (meaning data already approved for permanent retention), ask yourself if the information is reasonably believed to be necessary to perform your mission.

**PRACTITIONER'S TIP 8: (SLIDE 12)**
For Special Circumstances Collection, the Head of DIC or delegee must follow a 2-part process. First, determine the need for enhanced safeguards and, then identify and implement appropriate. measures.

**PRACTITIONER'S TIP 9: (SLIDE 13)**
USPI protections require collaboration between the intelligence professionals who handle USPI, the IT professionals who make it accessible, the legal professionals who advise, the privacy and oversight officials who help enforce the provisions, and the head of Component who's ultimately responsible for compliance. These items are auditable and should be integrated in your oversight program.

# Final Procedure 3 Takeaways

- **Responsibilities of Defense Intelligence Components**
  - Understand when Procedure 3 Applies & Key Terms
  - Know the Standard for Permanent Retention / Temporary Retention Periods and how they apply to the 4 Types of Collection
  - Note the rules for information disseminated to your Component
  - Apply Enhanced Safeguards, where applicable
  - Apply USPI Protections (Measures, Marking, Review) to limit access, tailor queries, take reasonable steps to audit access and queries, take reasonably steps to ensure effective auditing and reporting in information systems development or deployment, etc.
  - Document procedures and reasons for retaining USPI

# Procedure 3
# Retention of USPI

## Questions?

# Procedure 3
# Retention of USPI

## Back Up Slides

# Procedure 3
# Retention of USPI

## Sample USPI Markings

(U//FOUO) This product contains information concerning U.S. person(s) that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided, in accordance with the DoD Manual 5240.01 and Executive Order 12333. It should be handled IAW recipient's intelligence oversight and/or information handling procedures. Other U.S. person information may have been minimized. Should you require minimized U.S. person information, contact [REPLACE WITH NGA OFFICE/DIVISION/BRANCH/TEAM NAME], Secure [REPLACE WITH NGA OFFICE/DIVISION/BRANCH/TEAM NAME'S SECURE PHONE NUMBER], Commercial [REPLACE WITH NGAOFFICE/DIVISION/BRANCH/TEAM NAME COMMERCIAL PHONE NUMBER], OR DSN [REPLACE WITH NGA OFFICE/DIVISION/BRANCH/TEAM NAME DSN NUMBER].

USPI Marking for an Intel Product

(U) Domestic imagery obtained IAW Proper Use Memorandum (NUMBER); U.S. person(s) information deemed necessary for intended recipient to understand, assess, or act on the information provided IAW DoDM 5240.01 and E.O. 12333. This domestic imagery may only be used IAW a valid Proper Use Memorandum approved by NGA. This imagery may be used for law enforcement authorities only IAW applicable law, may not target U.S. persons, and may not be used for regulatory action. Removal of this caveat is prohibited. Questions can be addressed to NDRO@nscn.nga.smil.mil (SIPRNet) or NDRO@nga.ic.gov (JWICS).

USPI Marking with Domestic Imagery for an Intel Product

(U) This document contains information concerning U.S. person(s), which has been included consistent with applicable laws, directives and policies. Handle in accordance with recipient's intelligence oversight and/or information handling procedures.

USPI Marking for an Intel Briefing

# Procedure 3
# Retention of USPI

## Sample USPI Markings, cont.

Automated Systems - Disclaimer and Terms and Conditions

(U) The use of automated services provided by or through NGA for acquisition or collection of information concerning specifically identifiable U.S. person(s) and/or domestic imagery must be accomplished in accordance with the applicable NGA rules and instructions, as well as the rules and instructions of the user's sponsoring government organization, including rules concerning intelligence oversight and/or information handling procedures. For more information, see Terms and Conditions.

(U//FOUO) Terms and Conditions Notice: The following three paragraphs (Intelligence Oversight, U.S. Person Information, and Domestic Imagery and Overhead Persistent Infrared Data) must be included on every "Terms and Conditions Notice."
(U) Intelligence Oversight:
(U) The use of on-line services provided by NGA for acquisition or collection of information concerning specifically identifiable U.S. person(s) and/or domestic imagery must be accomplished in accordance with the applicable NGA rules and instructions, as well as the rules and instructions of the user's sponsoring government organization, including rules concerning intelligence oversight.
(U) U.S. Person Information:
(U) For members of the U.S. Intelligence Community, acquisition or collection of specifically identifying U.S. person(s) information must be accomplished in accordance with Executive Order 12333, as amended, and the sponsoring organization's Attorney General Guidelines. For Defense Intelligence Component (DIC) users, collection of information concerning specifically identifying U.S. person(s) also must be accomplished in accordance with DoD Directive 5240.1 and DoDM 5240.01, and any DIC implementing instructions or regulations. U.S. person information may include domestic imagery of property belonging to a U.S. citizen, a Permanent Resident Alien (PRA) or Lawful Permanent Resident (LPR), an unincorporated association comprised of more than 50% U.S. citizens, or PRA-LPR, and a wholly owned or majority held U.S. corporation not owned or controlled by a foreign government. It may include imagery of privately owned, non-federal, U.S. flagged vessels in domestic and international waters. Further, U.S. person rules may apply to property known to be owned by qualifying U.S. citizens, unincorporated associations, and corporations located on foreign territory.
(U) Domestic Imagery and Overhead Persistent Infrared Data:
(U) Users are responsible for ensuring a valid Proper Use Memorandum (PUM) is in place for any domestic imagery content for which it is required. NGA defines domestic imagery as imagery covering the land areas of the 50 United States, the District of Columbia, and the territories and possessions of the United States, and any adjacent waters to a 12-nautical-mile seaward limit of the land area.
(U) Users may contact NDRO via the appropriate system to obtain guidance concerning PUM requirements at either NDRO@nga.ic.gov, NDRO@nga.smil.mil or NDRO@nga.mil. NGA is not responsible for obtaining, maintaining, or tracking the use of PUMs as they relate to content exposed through the on-line services.

# DoD 5240.1-R Excerpt



C3. CHAPTER 3

PROCEDURE 3. RETENTION OF INFORMATION ABOUT UNITED STATES PERSONS

C3.1. APPLICABILITY

This procedure governs the kinds of information about United States persons that may knowingly be retained by a DoD intelligence component without the consent of the person whom the information concerns. It does not apply when the information in question is retained solely for administrative purposes or is required by law to be maintained.

C3.2. EXPLANATION OF UNDEFINED TERMS

The term "retention," as used in this procedure, refers only to the maintenance of information about United States persons that can be retrieved by reference to the person's name or other identifying data.

C3.3. CRITERIA FOR RETENTION

C3.3.1. Retention of Information Collected Under Procedure 2. Information about United States persons may be retained if it was collected pursuant to Procedure 2.

C3.3.2. Retention of Information Acquired Incidentally. Information about United States persons collected incidentally to authorized collection may be retained if:

C3.3.2.1. Such information could have been collected intentionally under Procedure 2;

C3.3.2.2. Such information is necessary to understand or assess foreign intelligence or counterintelligence;

C3.3.2.3. The information is foreign intelligence or counterintelligence collected from electronic surveillance conducted in compliance with this Regulation; or

C3.3.2.4. Such information is incidental to authorized collection and may indicate involvement in activities that may violate Federal, State, local, or foreign law.





C3.3.3. Retention of Information Relating to Functions of Other DoD Components or non-DoD Agencies. Information about United States persons that pertains solely to the functions of other DoD Components or Agencies outside the Department of Defense shall be retained only as necessary to transmit or deliver such information to the appropriate recipients.

C3.3.4. Temporary Retention. Information about United States persons may be retained temporarily, for a period not to exceed 90 days, solely for the purpose of determining whether that information may be permanently retained under these procedures.

C3.3.5. Retention of Other Information. Information about United States persons other than that covered by paragraphs C3.3.1. through C3.3.4., above, shall be retained only for purposes of reporting such collection for oversight purposes and for any subsequent proceedings that may be necessary.

C3.4. ACCESS AND RETENTION

C3.4.1. Controls On Access to Retained Information. Access within a DoD intelligence component to information about United States persons retained pursuant to this procedure shall be limited to those with a need to know.

C3.4.2. Duration of Retention. Disposition of information about United States Persons retained in the files of DoD intelligence components will comply with the disposition schedules approved by the Archivist of the United States for the files or records in which the information is retained.

C3.4.3. Information Acquired Prior to Effective Date. Information acquired prior to the effective date of this procedure may be retained by DoD intelligence components without being screened for compliance with this procedure or Executive Order 12333 (reference (a)), so long as retention was in compliance with applicable law and previous Executive orders.