PROC 2 FAQs

1. DoDM 5240.01, paragraph 3.2.c.(9), "Personnel Security," enables the intentional collection of U.S. person information (USPI) when the "information is arising from a lawful personnel security investigation." In the DoD, personnel security investigations are normally conducted by dedicated security personnel, not intelligence personnel. Does paragraph 3.2.c.(9) enable intelligence personnel to support security personnel in conducting these investigations? If so, does this authority extend to collecting background information on family members and other people associated with the subject of the personnel security investigation?

Answer: Paragraph 3.2.c.(9) allows a Defense Intelligence Component to intentionally collect USPI arising out of a lawful personnel security investigation, if the information is otherwise reasonably believed to be necessary for the performance of an authorized intelligence mission or function assigned to the Component. As the question observes, personnel security investigations are normally conducted by dedicated security personnel; these personnel execute their investigatory functions under authorities distinct from E.O. 12333, and follow the policies and procedures established in DoD issuances including DoDI 5200.02 and DoDM 5200.02. Defense Intelligence Component personnel providing support to security personnel would do so under those non-E.O. 12333 authorities. Such support could include discovery of background information on family members and other people associated with the subject of the personnel security investigation.

2. Does DoDM 5240.01, paragraph 3.2.c.(4)(c) authorize DoD CI personnel to intentionally collect U.S. person information on people who are in the U.S. and are believed to be homegrown violent extremists, even in the absence of a specific connection to foreign terrorists?

Answer: The term "homegrown violent extremist" is a colloquial term that is not officially defined in DoD policy. DoDM 5240.01, paragraph 3.2.c.(4)(c) authorizes intentional collection of U.S. person information (USPI) if the information is reasonably believed to constitute counterintelligence (CI) and the U.S. person is an "individual, organization, or group reasonably believed to be acting for, or in the furtherance of, the goals or objectives of an international terrorist or international terrorist organization, for purposes harmful to the national security of the United States." Such an individual may not have a specific connection to a particular foreign terrorist group, but there must be a "reasonable belief" that he or she is acting to further the goals of an international terrorist or international terrorist group and is acting for purposes harmful to U.S. national security. Depending on the facts, such a belief may be based in whole or in part on the person's engagement with terrorist groups' propaganda on the Internet or social media. It is the responsibility of DoD CI elements to investigate all international terrorist threats against the DoD in the U.S. and overseas. These CI elements have the mission to investigate active duty military members of their Service, DoD civilian personnel or DoD Contractors who may be engaged in these activities that threaten the security of DoD. CI investigations of persons in the U.S. other than active duty military members must be coordinated with the Federal Bureau of Investigation when conducted inside the U.S. and coordinated with the Central Intelligence Agency when conducted outside the U.S.

3. DoDM 5240.01, paragraph 3.2.c.(8) authorizes the intentional collection of U.S. person information (USPI) if the "information is about persons in contact with sources or potential sources, for the purposes of assessing the suitability or credibility of such sources or potential sources." What kind of collection may take place with respect to these U.S. persons? Might it include electronic surveillance? Would it be possible for collection to take place regarding a U.S. person because they have a social, familial, or professional relationship with someone who is or may be a source, or because they are "friends" with a potential source on a social media site?

Answer: The fundamental requirement for any collection of USPI is that a Defense Intelligence Component (DIC) may intentionally collect USPI only if the information sought is reasonably believed to be necessary for the performance of an authorized foreign intelligence or counterintelligence mission or function assigned to the DIC. DoDM 5240.01, paragraph 3.2.c.(8), does not assign any mission or function to a DIC or otherwise authorize the use of specialized collection techniques, such as electronic surveillance or concealed monitoring. Federal surveillance laws and other provisions of DoDM 5240.01 govern special collection techniques (e.g., electronic surveillance, concealed monitoring, etc.), including DoDM 5240.01 paragraph 3.2.f.(3), which provides that Defense Intelligence Components will use the least intrusive collection techniques feasible within the United States or directed against U.S. persons abroad. Accordingly, an associate of a potential source might be subject to electronic surveillance, but only if the DIC has the necessary information to satisfy the requirements of DoDM 5240.01, Procedure 5 and the Foreign Intelligence Surveillance Act. Subject to the foregoing, a Defense Intelligence Component may collect information about people with a social, familial, or professional relationship with someone who is or may be a source, *provided that* the purpose is to assess the suitability or credibility of the source or potential source. The provision allows a DIC to follow normal leads to assess a source or potential source. For instance, if a source has said that he is in touch with person X who is involved in ordinary international business activities, it may be appropriate to learn more about person X to see if this is in fact the case. Similarly, if information about a potential source's association with a group is revealed, it would be relevant for the DIC to gather information about that group to determine if it is associated with a foreign government. Because of the requirement that a source or potential source be "in contact with" the other person, a DIC could not use this provision to collect information about the friends or other contacts of the other person, unless they too were "in contact with" the source or potential source.

4. When preparing an intelligence briefing containing public comments made by a U.S. government official during a press conference, is it permissible to include the official's name in the briefing? One interpretation is that it is okay to use the official's title, but including the name of the official constituted U.S. person information (USPI) and violated DoD Manual 5240.01. Another interpretation is that using the official's name is allowed under Category 2. Which is correct? Does the inclusion of the name require that the briefing be marked as containing USPI?

Answer: In accordance with the definition of USPI in the Glossary of DoDM 5240.01, the title of the U.S. official is identifying information and must be protected in accordance with

the Procedures. In the case you cited above, the information is releasable to any person or entity because it is publically available, but should be marked as USPI.

With regard to marking intelligence containing USPI, see DoDM 5240.01, Paragraph 3.3.f.(2): "Marking Electronic and Paper Files. Defense Intelligence Components will use reasonable measures to identify and mark or tag files reasonably believed or known to contain USPI. Marking and tagging will occur regardless of the format or location of the information or the method of storing it. When appropriate and reasonably possible, Components will also mark files and documents containing USPI individually. In the case of certain electronic databases, if it is not reasonably possible to mark individual files containing USPI, Components may use a banner informing users before access that they may encounter USPI."

5. If information is provided to a DoD Component by a Federal agency that is not a member of the Intelligence Community(IC), how is this information evaluated for purposes of Permanent Retention as per Paragraphs 3.3.d. and 3.3.e. of the Manual?

Answer: Information received from any source that is not an IC element is considered to be collected upon receipt and must meet the requirements in Procedure 2 for collection and Procedure 3 for retention.

Answer: Certain operational activities must comply with intelligence guidelines and oversight requirements. Revised policy related to "intelligence-related activities" is being considered for inclusion in DoD Directive 5240.01.

6. Can there be a better, more consistent determination of what is and what is not USPI? For example, is a U.S. passport number USPI?

Answer: USPI is information that is reasonably likely to identify one or more specific U.S. persons. USPI may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons. In this case, a U.S. passport number is reasonably likely to identify a U.S. person and is USPI. Ultimately, determining whether information is reasonably likely to identify one or more specific U.S. persons in a particular context may require a case-by-case assessment by a trained intelligence professional or legal counsel.

7. How do the procedures in DoD Manual 5240.01 apply to intelligence reports produced by foreign partner intelligence services?

Answer: Usually, when a Defense Intelligence Component receives an intelligence report produced by a foreign partner nation, the information is considered "collected" upon receipt by the Defense Intelligence Component and must be evaluated for permanent retention in accordance with DoDM 5240.01, paragraphs 3.3.c.(3) and 3.3.e., and protected in accordance with DoDM 5240.01, paragraph 3.3.f.

8. May I collect, retain, and disseminate publicly available U.S. person information?

Answer: Since publicly available U.S. person information falls within one of the 13 categories in DoDM 5240.01, paragraph 3.2.c., it may be intentionally collected if the information sought is reasonably believed to be necessary for the performance of an authorized intelligence mission or function. Regardless of whether the information is intentionally or incidentally collected or voluntarily provided, it must be evaluated, after collection, for permanent retention in accordance with DoD Manual 5240.01, paragraph 3.3.e. If the USPI is properly collected and retained, it is eligible for dissemination in accordance with DoD Manual 5240.01, paragraph 3.4.c.

9. Is a *Raytheon Corporation* radar and its specific parameters considered USPI when identified in an intelligence database as a system manufactured by *Raytheon*?

Answer: No. In this case, *Raytheon* is used "in a descriptive sense" as the manufacturer of the product, and is excluded in accordance with the definition of USPI in the DoDM 5240.01 glossary.