This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.
FIXING LEAKS

ASSESSING THE DEPARTMENT OF DEFENSE’S APPROACH TO PREVENTING AND DETERRING UNAUTHORIZED DISCLOSURES

JAMES B. BRUCE ■ W. GEORGE JAMESON

Prepared for the Office of the Secretary of Defense
Approved for public release; distribution unlimited
Summary

Introduction

Recent unauthorized disclosures (UDs) of classified information, particularly those to the public media that put sensitive operations and intelligence sources and methods at risk, have highlighted the inadequacy of extant law and policy to address the causes of and remedies to such damaging disclosures. In response to this situation, the Under Secretary of Defense for Intelligence (USD(I)) has initiated a new series of comprehensive measures, all of which are encapsulated within a Strategic Plan designed to address this heretofore intractable issue. The Plan was developed by a Department of Defense (DoD) Unauthorized Disclosures Working Group (UDWG) assembled in response to direction from the Defense Security Enterprise (DSE) Executive Committee (EXCOM) and subsequent amplifying tasking from the Under Secretary of Defense for Intelligence. Further, pursuant to the recommendations of the UDWG, OUSD(I) established an Unauthorized Disclosures Program Implementation Team (UD PIT) to oversee Strategic Plan implementation and its incremental improvement. More specifically, the UD PIT, endorsed by the Defense Security Enterprise Advisory Group (DSEAG), was established to prevent and deter the unauthorized disclosure of classified information by all personnel through the implementation of the UD Strategic Plan.

With a view toward enhancing its odds of success and to discover any deficiencies that, if remedied, could improve the potential effectiveness of the overall program, OUSD(I) asked the RAND Corporation to provide an outside perspective in assessing the program concept
and its early implementation. Specifically, RAND was asked to monitor and assess the potential for effectiveness of the UD PIT initiative to stem UDs of classified information and to make recommendations as needed.

To meet this objective, RAND assigned two senior researchers with demonstrated expertise in UDs to support OUSD(I), the Deputy Under Secretary for Defense (DUSD) for Intelligence and Security, and the UD PIT on a part-time basis to review and assess UD Strategic Plan implementation and its early effectiveness. The researchers also engaged with appropriate personnel in DoD and in the Intelligence Community (IC) to obtain perspectives on how to improve the DoD’s UD Strategic Plan content, framework, and overall implementation.

**Observations on the UD PIT**

The UD PIT’s implementation of the UD Strategic Plan has made important and discernible progress toward its main objectives. These include clarifying reporting procedures and sanctions; achieving gains in improving awareness and training; and better integrating key supporting functions such as counterintelligence (CI), law enforcement, and legal staff. The UD PIT is exerting effective leadership in implementing a significant and comprehensive Strategic Plan that extends broadly throughout DoD. It is building a new and untried infrastructure of personnel and mechanisms to address UDs. And it is setting clearer boundaries on what is impermissible behavior in terms of the disclosure of classified information to those unauthorized to receive it.

These early successes are attributable to several factors, including that the initiative is driven by the Secretary of Defense and is top-down in nature; that the plan is well conceived and being ably executed; and that there is a broad and growing (if uneven) appreciation in the department for the seriousness of the issue at hand and the need to address it effectively.

While the early successes thus far are notable, they are also partial, fragile, and by no means permanent. Preventing and deterring the unauthorized disclosure of classified information in an
organization as large as DoD is no easy task. Even if the UD Strategic Plan were fully implemented, further efforts would be necessary to deal with the most serious part of the problem—significant classified leaks to the media, which feed voracious foreign intelligence services. To attack this tougher issue—and the one most resistant to durable solutions to the larger UD problem—the UD PIT should continue its implementation activities, but it should direct more-focused attention to establishing an end-to-end accountability process that will help transform the current “leaks-tolerant” culture that exists within DoD.

As such, addressing the problem requires overcoming both strategic and tactical obstacles. In terms of strategic obstacles, the enormity of the UD challenge is defined by three historically daunting issues that defy simple fixes: (1) media leaks have many causes but few feasible and effective solutions; (2) there is a longstanding organizational culture in DoD that treats leaking classified information to the media as nearly risk-free, which suggests to some that the behavior is acceptable; and (3) to be fully effective, remedies must address the full range of security, classification, and particularly UD-related behavior, from initial UD identification through the imposition of effective penalties for violations.

- **Many causes, hard fixes.** Of the four main factors identified in the 2005 Weapons of Mass Destruction (WMD) Commission Report as making the leaks problem nearly intractable, only one has changed: The political will to act against leakers is no longer wholly absent. The other three longstanding factors—using UDIs to influence policy, the difficulty of identifying leakers, and outdated or overly narrow laws that make leaks prosecutions extremely difficult—have remained the same. Thus, any successful initiative to stem UDIs must both capitalize on the recently improved political climate to reduce them and also take full account of the three remaining obstacles to controlling classified leaks. The study recommendations address these obstacles.

- **Culture of leaking.** There are many motives and reasons underlying classified leaks, including political motivations to leak to the press, the variability of classification standards across DoD
and other departments and agencies, and the everyday practical difficulty of protecting classified information. All of these nourish a culture that tolerates leaking. So few leakers ever get caught and punished, it is commonly understood that the incentives for leaking almost always outweigh the penalties. As far as the leaker is concerned, if there are no appreciable penalties and only advantages, then why stop? Solutions that will gain traction over the longer term are those that will effectively address this culture of permissiveness.

- **Establishing accountability.** A comprehensive end-to-end accountability process entails four major phases: (1) identifying and officially recording every occurrence of a UD, (2) taking or assigning “ownership” of organizational responsibility to see a case through to closure, (3) identifying who leaked the classified information, and (4) holding the leaker fully accountable for violating regulations and laws. The penalties for leaking classified information—which are too rarely applied—include a variety of administrative sanctions, civil penalties, and, in the most-serious cases, criminal prosecution.

Beyond these strategic obstacles that contribute to the very existence of UDs, there are also some important tactical obstacles the UD PIT must confront in sustaining its current accomplishments.

- **Addressing UD PIT focus issues.** Successfully addressing the unauthorized disclosures problem requires carefully calibrating the focus of the UD PIT efforts. The current focus risks being both too broad and too narrow. It is too broad in that it encompasses a wide scope of UDs—both intended and unintended, including everything from minor security infractions and other lesser breaches to deliberate leaks to the media of highly classified information. Such leaks sometimes occur in large volumes, such as WikiLeaks, or are program-jeopardizing, such as the recent disclosures about the National Security Agency collection of U.S. phone metadata and email records. The most-significant UDs require greater attention. On the other hand, the UD PIT
approach is too narrow in that it focuses mostly on identification and reporting. These activities must be complemented by other, equally significant tasks, such as assigning responsibility and ownership for acting on the reported UD, seeing the action through all the needed steps to establish full accountability and appropriate sanctions for offenders, and bringing it to closure.

- **Prioritizing preventive security.** Because a key goal of the Strategic Plan is to prevent UDs, it is important to identify steps where security can act before leaks occur. The UD PIT’s efforts would benefit from giving added emphasis to a review of DoD measures that will ensure clarity and effective implementation of existing requirements, as well as determining where new measures could improve the vetting process. Specifically, the following three areas require attention: existing standards for security clearances, rules to limit unsupervised access by even security-cleared personnel to the most-sensitive information, and timely electronic monitoring capabilities that can identify insider threats and other attempts to obtain unauthorized access.

- **Clarifying the language and guidance in addressing UDs.** The language and guidance addressing UDs are often unclear and inconsistent, which argues for the UD PIT taking steps to ensure that DoD directives, manuals, and other issuances—and guidance from senior officials—are clear and consistent.

- **Creating metrics.** While much attention is given to numbers of UDs, little has been paid to those metrics that focus on results or that can help with understanding what will deter and prevent UDs. DoD’s metrics effort is still nascent. Until the UD PIT is able to deliver a richer level of detail, there will be few actionable insights that reach beyond identifying and tracking UDs. Similarly, there is a need to establish an analytic focus that addresses the causes of leaks, their consequences, and how to prevent them.

- **Addressing CI and security issues.** The UD PIT must resolve sensitivity issues, ambiguities, and even resistance where CI interests arise regarding the obligation of all DoD elements, including CI, to formally report UDs to the Director of Security Policy and Oversight, OUSD(I), in a timely manner. Additionally, a major
security issue is the adequacy of vetting of U.S. government and contractor personnel for access to classified and sensitive information, as well as the adequacy of day-to-day security measures to detect insider threats and oversight of their implementation. For example, both Edward Snowden and Bradley Manning are responsible for significant UDIs that might have been prevented; both had evinced behavioral issues that, in retrospect, should have raised questions about their suitability for access to classified information.

• **Making UD process improvements:** Organizational and management issues related to the authority and functioning of the UD PIT require clarification and possible changes to improve direction and component responsiveness.

• **Having more outreach and integration:** The UD effort has made considerable headway, and the OUSD(I) Security Policy and Oversight Directorate and, increasingly, UD PIT membership have been suitably engaged, but greater UD PIT outreach and attention to other major stakeholders with equities in addressing the UD problem will leverage gains and effectiveness.

**Recommendations**

The 22 recommendations offered in this report are keyed on sustaining the successes that the UD PIT has already achieved. They also seek to enhance and focus UD PIT efforts to address any uncompleted actions, shortfalls, and other areas of the DoD UD Strategic Plan that warrant priority attention. They span UD PIT management, culture and accountability, policy and new initiatives, and studies and outreach.

**UD PIT Management**

1. **Hold your ground.** Revalidate the UD Strategic Plan and the importance of the UD PIT. Maintain and consolidate the gains already established.
2. **Expand your ground.** Grow the UD initiative through a recalibrated and even more ambitious agenda, as well as through greater DoD-wide senior-level oversight and direction.

3. **Sustain the top-down approach.** With the recent transition in Defense Secretaries, ensure that the top-level priority and support assigned to the UD initiative by the previous Secretary is reinforced and sustained by the new leadership.

4. **Enhance UD PIT authority.** Empower UD PIT members within their components and establish a Senior Executive Service (SES)–level UD steering group, possibly a subgroup of the DSE EXCOM, to which the PIT should regularly report.

5. **Focus on the significant UDs.** With prioritization guidance worked out by the Program Management Office (PMO), direct the PIT’s focus to the most-serious classified disclosures to the media.

6. **Establish metrics to track results.** After counting the numbers of UDs, a more granular system of categorizing them and tracking end-to-end results is needed to better evaluate the performance of the PIT and PMO in accomplishing their mission.

**Culture and Accountability**

7. **Connect culture change with UD results.** Establishing full UD accountability by identifying leakers and applying sanctions will promote the realization that leakers will be caught and punished.

8. **Ensure end-to-end accountability for results.** The PIT should ensure that full ownership of every serious UD is assumed or assigned, that accountability is established as offenders are identified and adjudicated, and that appropriate sanctions are implemented before any serious case is brought to closure.

9. **Energize the three-track system.** Clarify policies, directives, and guidance to help managers understand their authorities and responsibilities to ensure that accountability is established as identified offenders are punished for violations.
10. **Facilitate compliance through a reasonable approach.** An effective system will facilitate, not inhibit, compliance; sanctions must be timely, visible, meaningful, and fair.

11. **Prioritize and deliver quality UD training and education.** A workforce that is more knowledgeable and alert to UDs will get on board, improve compliance, and support culture change.

**Policy and New Initiatives**

12. **Align UD language with PIT goals.** Ensure language clarity and consistency in all relevant DoD documents, directives, manuals, and official issuances—and along the full range of departmental authorities.

13. **Resolve classification and sensitivity barriers.** Ensure that, regardless of sensitivity, UDs involving CI, the Inspector General (IG), law enforcement, Sensitive Compartmented Information (SCI), Special Access Program (SAP), and Alternative Compensatory Control Measures (ACCM) are reported to the Security Policy and Oversight Directorate in a timely manner.

14. **Review Security Vetting for Classified Access.** The UD PIT should elevate the importance of security vetting in its Strategic Plan and help lead an effort to review and reform such DoD security measures that should include a reliable and predictive evaluation of security trustworthiness.

15. **Leverage technology.** Review available technologies and develop or adapt new technologies that will enhance the implementation of the Strategic Plan and related initiatives for training, analytic, and investigatory purposes, as well as the protection of information and systems.

16. **Lay the foundation for comprehensive leaks legislation.** Identify promising attributes of more-effective laws addressing UDs, brief the Armed Services and Intelligence Committees on the Strategic Plan, and build support among those committees, the White House, and others for submitting draft leaks legislation.
Studies and Outreach

17. **Conduct a comprehensive study of UDs.** Such a study should assess causes, consequences, and correctives that will help in understanding UDs, enhancing prioritization efforts, and sustaining the effectiveness of the UD program over the long haul.

18. **Study ways to improve the identification of leakers (Step 3 of the end-to-end accountability process discussed in Chapter Two).** Review available analytic, technological, collaborative, and other investigatory tools and develop new ones to identify leakers.

19. **Study ways to improve the implementation of sanctions when leakers are identified (Step 4 of the end-to-end accountability process discussed in Chapter Two).** Review the three-track sanctions options—administrative, civil, and criminal—for maximum applicability.

20. **Expand outreach.** The UD PIT should take advantage of the expertise and lessons learned from the numerous organizations outside of USD(I) that have interests and equities in supporting the PIT UD goals.

21. **Seek closer alignment with the ODNI and other IC approaches to UDs.** Ensure that separate IC and DoD action tracks are appropriately synchronized with each other.

22. **Engage the Inspectors General.** The role of the IG in supporting the top-down initiative should be defined, with particular emphasis on identifying systemic problems in the implementation of the Strategic Plan and other UD-related mechanisms, practices, and shortcomings, as well as investigations into which IG authorities may be valuable in crossing organizational lines.