# Enabling Mission Success by Avoiding Over-Classification

by Major Daniel Jarvis

## Introduction

Military intelligence professionals safeguard classified information daily. We limit access to the information using technical and physical methods and applying personnel and administrative control measures.[1] By their very nature, our military occupational specialties ingrain the task of securing information, reinforced through the framework of our duties. This instinct, developed in training and honed during operations, tends to cause many individuals to apply automatically the highest classification possible. This tendency can result in an unnecessary hindrance to the organizations we serve. Guarding information in order to deny access to the greatest extent possible is a detriment to mission accomplishment. Instead of using over-classifications to protect information, the intelligence professional has a duty to ensure operational success through applying the proper markings, sharing appropriately, and *granting* access to the right people.

## A Natural Inclination to Protect

Service members across all warfighting functions take recurring, mandatory training emphasizing the protection of information against adversaries. It is no surprise that, when dealing with the greatest amount of classified information, the intelligence community believes it has the obligation to be the leader in the effort to safeguard it. The tendency of improperly trained individuals is to classify at the highest possible level within the system used.

Typical analysts' duties include research and data collection from a multitude of classified sources to create situational understanding for commands and make predictive analysis based on reporting and trends. These individuals are expected to have adequate knowledge of the subject matter, the appropriate classification guidelines, and the purpose of their tasks while compiling information for multiple products with derivative classifications.[2] For the sake of saving time and effort, the majority of analysts use the highest overall classification from the source data and label their own product similarly without fully knowing, or asking, which specific portions require the classification. They also tend to label electronic communication at the level of the system they are using instead of the level of information they are sending. Many individuals automatically label every SECRET Internet Protocol Router Network email as "SECRET//NOFORN" [not releasable to foreign nationals] without regard for the message itself. This ingrained default mindset is based on goodwill—doing our job to protect information that could cause damage to national security—but improper markings often tie our own organization's hands more than necessary by preventing the information from reaching the appropriate end user.

This lack of clarity or specificity when passing information is not only a bad habit but is also contrary to guidance from the Office of the Director of National Intelligence. The guidance recommends labeling information at the lowest possible level because over-classification "restricts information sharing [and] hinders the optimal use of intelligence information in support of national security and foreign policy goals."[3] The bottom line with creating products containing derivative classification is to use specificity and ask for clarification when necessary. This specificity includes the use of classification markings on individual lines or paragraphs within products or communications to identify precisely what part of the information requires the access and dissemination control. If a person is unsure of why an overall classification exists, he or she may apply the safe practice of using the highest label, but the best option is to verify with the originator.

## Tragic Lessons from History

While the following lesson from history is not an example of over-classification of intelligence, it is an important

example of over-classification of information. Over-classification and the related inability to share information have led to issues ranging from unnecessary operational obstacles to some of the worst disasters in military history. In 1945, the USS *Indianapolis* participated in one of the most highly classified operations of World War II as it delivered components of the atomic bomb for use against Japan. Once the cargo arrived safely at Tinian, the USS *Indianapolis* stopped at Guam before continuing unescorted for Leyte when two torpedoes from a Japanese submarine struck it shortly after midnight on 30 July. It sank in less than 15 minutes. Hundreds of Sailors who did not initially go down with their ship died within the next three days after vainly trying to survive in the shark-infested waters, experiencing dehydration and hysteria. A passing pilot randomly spotted and rescued the survivors on the evening of 2 August.[4] The Navy, unaware the ship had sunk, had not begun an official search. Although the primary reasons for the tragic lack of a deliberate search and the unnecessarily delayed rescue were related to defects in scheduling, routing, tracking, and escort procedures, issues surrounding the classification of information also contributed to the disaster.[5]

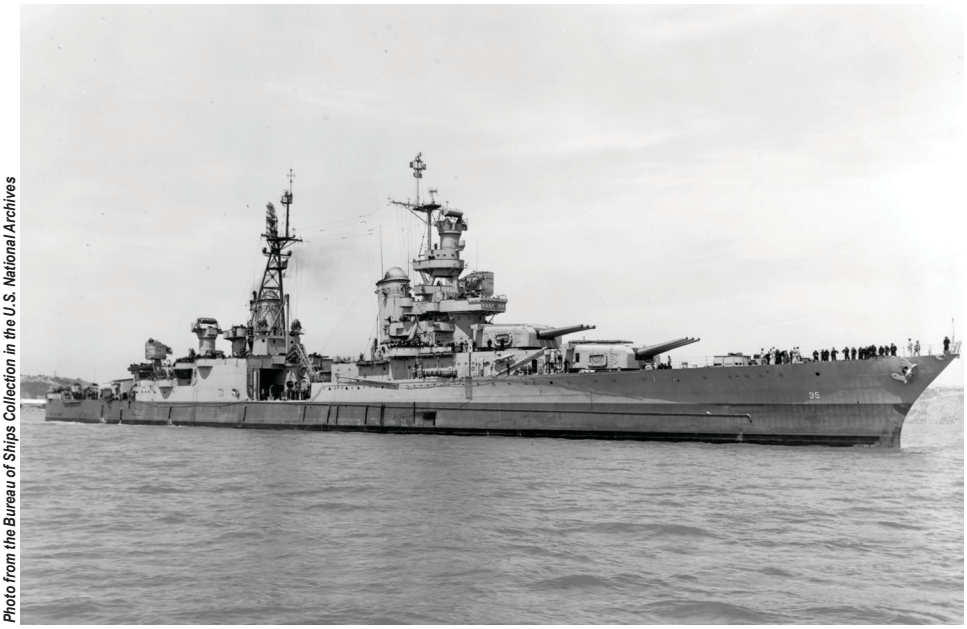

*Photo from the Bureau of Ships Collection in the U.S. National Archives*

**The USS *Indianapolis* off the Mare Island Navy Yard, CA, 10 July 1945, after her final overhaul and repair of combat damage.**

The extremely sensitive nature of the USS *Indianapolis'* classified mission was so protected that the ship's purpose was known to only a limited number of top naval officials, and its mere presence in the area was known to only as few people (beyond the crew) as necessary for logistic and operational reasons. Hours after the sinking, when naval intelligence received reporting from enemy sources of the successful Japanese attack in the approximate scheduled location of the USS *Indianapolis,* analysts dismissed it as false reporting, uninformed the ship was actually there.[6] Due to the overly sensitive approach to protect the operation beyond the classified portion of the mission, the Navy lost hours of critical time to save lives. Highlighting what may happen when necessary end users are denied access to information, the blanket over-classification of every aspect related to the USS *Indianapolis'* mission complicated the situation and contributed to turning an unfortunate operational loss into a tragedy.

Further still, the inability to share intelligence has also proven disastrous at a strategic level. Now engrained in our national narrative, the infamous and seemingly unprovoked attack against the U.S. Pacific Fleet at Pearl Harbor catapulted the Nation into World War II. Although military and political leaders were aware of an existing threat and even received reports of a probable attack by the Japanese, the inability to predict the "when, where, or how" prevented the necessary preparations. Competitive interest, bureaucratic disorder, distrust, misunderstanding, and lack of communication between intelligence services prevented collaboration. National security suffered as a result. It is almost incomprehensible that this type of event could happen twice to the same nation in a 60-year span, but it did. In the time leading up to September 11, 2001, organizations within the U.S. intelligence community were not collaborating—a grave mistake to avoid in the future.

## Sharing Properly

Learning how to share properly is a critical aspect to classifying information. Most likely, the originator will correctly classify a document given their subject matter expertise, but analysts must be aware of their ability to properly challenge the classification if necessary. According to regulations, if any authorized user has probable reason to believe improper or unnecessary classifications exist, they can communicate their concern to the security manager.[7] It is the intelligence professional's charge to use the standard prescribed processes and correct justifiable errors. This enables information to reach the appropriate level required for action, including when partnered with outside agencies or even foreign services.

A key tool available to the analyst is the Foreign Disclosure Office. Analysts need to know how to contact the office to

create appropriately sanitized and releasable information. Since we were an infantry battalion S-2 section preparing for a deployment consisting of retrograde operations and handover with Afghan forces, personnel from our section attended Foreign Disclosure Office training, specifically to enable the unit's internal ability to share releasable information with partnered forces. After the initial weeks in country, the commander directed leaders to share all knowledge and information with our partners, and the criticality of this skillset quickly became apparent. One company commander's initial misinterpretation of this guidance to share nearly led to an unauthorized disclosure of classified information. Trained personnel caught the error and corrected it before any security incident occurred. To enable operations moving forward, the ability of our intelligence section analysts to create two versions (one shareable and one not) for every disseminated intelligence estimate fostered success for both the organic companies and their partnered Afghan elements. Achieving successful operations with host-nation forces in the lead called for intelligence sharing; doing so correctly required the battalion intelligence section to create sanitized products and inform leaders on the proper procedures for handling them.

**The Foreign Disclosure Officer and Foreign Disclosure Representative**

The foreign disclosure officer (FDO) is a formally designated individual authorized and tasked to plan for, recommend, and effect the disclosure of classified military information (CMI) and controlled unclassified information (CUI) to an authorized representative of a foreign government or international organization. The FDO makes disclosure determinations based on the policies, directives, and laws that govern national disclosure policy and the release of classified information. The FDO provides this service to the command and staff and to assigned, attached, and supporting agencies, allies, and other multinational partners.

The FDO can be either a uniformed member of the staff or a Department of the Army (DA) Civilian. FDO responsibilities include, but are not limited to—

- Informing/advising the commander and staff on the impact and implications of current delegated disclosure authorities by country, category of information, and classification level on mission requirements.
- Advising the commander and staff on the recommended number and location of foreign disclosure representatives (FDRs) based on mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC).
- Directing the information production requirements efforts within the organization for all categories of CMI/CUI to ensure maximum disclosure to unified action partners.
- Coordinating for the authority and permission to disclose information originated outside the organization.
- Developing and promulgating foreign disclosure guidance for deployments, exercises, training events, and official foreign visits/visitors (including exchange and liaison officers).
- Ensuring unit and organizational compliance with AR 380-10, *Foreign Disclosure and Contacts with Foreign Representatives.*

An FDR is an individual designated in writing who assists, advises, and makes recommendations to the FDO on disclosure matters. FDRs can be either DA members or Army-employed contractor personnel.

In addition to making releasable products for combined operations, the correct labeling of classified information further enables communication among cleared planners. This is more evident in the management of special access programs (SAPs). SAPs are specially compartmented capabilities used to support commanders' efforts that demand stringent access restrictions. Their control is managed down to the individual capability and is available to an extremely limited audience of planners and command authorities. Each authorized user is responsible for the proper and accurate marking of products and communications relating to these capabilities. With such stringent controls of highly sensitive information, one could assume the safest practice of protection is using the highest available classification as a "catchall" safeguard; again, even with increased sensitivity, this is the improper approach. Over-classifying in a compartmented environment unnecessarily further restricts an already narrow audience of planners. It is even possible to accidentally deny access to the intended authorized end users. Furthermore, access to SAP planning systems and facilities is often limited. It consequently becomes the SAP manager's responsibility to properly share information at the lowest possible classification to ensure understanding and planning happen at all appropriate levels. For example, even though the capability itself may require SAP levels of security, the effects may be transmittable over top secret networks or broader operations for cleared persons at the secret level. Security managers are responsible for enabling successful planning efforts, applying as much scrutiny as when they safeguard the information or capability.

## Getting the Right People Access

Ensuring operational success from an intelligence perspective is more about getting the right people permission, not simply denying access. Planners must principally comprehend the why of their efforts. Understanding the commander's intent and desired end state is essential to developing intelligence support to operations. This allows

intelligence professionals to help commanders and staffs visualize the operational environment and make command decisions. A major challenge to this is the integration of key staff elements during the military decision-making process, collection operations, targeting, and assessments.[8] Often, intelligence planners' clearance and access exceed that of other staff members incorporated with these efforts. In addition to safeguarding information from spillage or disclosure, intelligence professionals must help determine if granting additional key planners access better enables operations.

Sometimes decision makers have access to information without enough individuals cleared to support the planning and staff work required. This occurs when granting access to a limited number of billets is based primarily on duty title, especially for sensitive compartmented information, alternate compensatory control measures, or special access requirements. If such a situation exists, the justification cannot be "that is the way it has always been"; the situation cannot remain unchallenged. Charged with getting the right people access, intelligence planners must determine if a need-to-know exists beyond predesignated billets to enable planning and operations.

Once the right people have the proper authorizations, they should be empowered to use their access to benefit the organization. Challenges associated with newly indoctrinated individuals include locating an available workspace within the appropriately cleared facility, establishing network connectivity with an account at the new classification levels, and understanding the purpose for gaining access. Security managers must take the extra step in letting people know *why* they are being read on to particular programs or caveats and how they can specifically contribute to planning. Maybe this includes explaining the procedures for nominating other persons for access who can provide additional benefits to planning efforts. Maybe they are serving in a unified organization and the person capable of providing the greatest benefit is a non-U.S. partner from an allied nation. The list of potential challenges is open ended, but if the reasons are justifiable, the solution to all of them is to ask through appropriate channels. Competent staff members do not stop at the first "no"; instead, they look for the answer. We must tell commanders how they can, not how they cannot.

## Conclusion

This is by no means a suggestion to reduce the emphasis placed on the protection of classified information. It is a call to ensure intelligence professionals place just as much, if not more, attention to ensuring mission accomplishment. Maintaining current knowledge of classification guidelines and procedures, understanding the processes to share information appropriately, and seeking to gain access for the right people are essential responsibilities of the intelligence planner. Properly classifying information can be tedious, time consuming, and difficult. It may be quicker to opt for the easy choice and over-classify, but it is the obligation of intelligence professionals to take the "hard right" and enable our organization's success.

**Endnotes**

1. Department of Defense, Department of Defense Manual 5200.1, *DoD Information Security Program: Protection of Classified Information, Volume 3* (Washington, DC: U.S. Government Publishing Office [GPO], February 24, 2012), 14. Change 2 was issued on March 19, 2013.

2. Department of the Army, Army Regulation (AR) 380-5, *Department of the Army Information Security Program* (Washington, DC: U.S. GPO, 29 September 2000), 7.

3. Office of the Director of National Intelligence, *Principles of Classification Management for the Intelligence Community,* April 4, 2017, 2, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2017/item/1745-the-principles-of-classification-management-for-the-intelligence-community.

4. "The Sinking of USS *Indianapolis*: Navy Department Press Release, Narrative of the Circumstances of the Loss of USS Indianapolis, 23 February 1946," Naval History and Heritage Command website, accessed 24 October 2019, https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/s/sinking-ussindianapolis/narrative-of-the-circumstances.html.

5. Sam Cox, "Lest We Forget: USS Indianapolis and Her Sailors," *The Sextant* (blog), Naval History and Heritage Command, August 24, 2017, http://usnhistory.navylive.dodlive.mil/2017/08/24/lest-we-forget-uss-indianapolis-and-her-sailors/.

6. "The Sinking of USS *Indianapolis*."

7. Department of the Army, AR 380-5, *Information Security*, 13.

8. Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: U.S. GPO, 31 July 2019), 5-2.

**Reference**

Department of the Army. Army Regulation 380-10, *Foreign Disclosure and Contacts with Foreign Representatives*. Washington, DC: U.S. GPO, 14 July 2015.

*MAJ Daniel Jarvis is the United States Forces Korea Integrated Joint Special Technical Operations Branch Chief and intelligence planner. He is a graduate of the Counterintelligence Officers Course and completed the Department of Defense Sensitive Compartmented Information Security Officers Course. His previous assignments include battalion S-2 and company commander, and he has deployed to Iraq and Afghanistan. He holds a master of arts degree in intelligence studies from American Military University.*