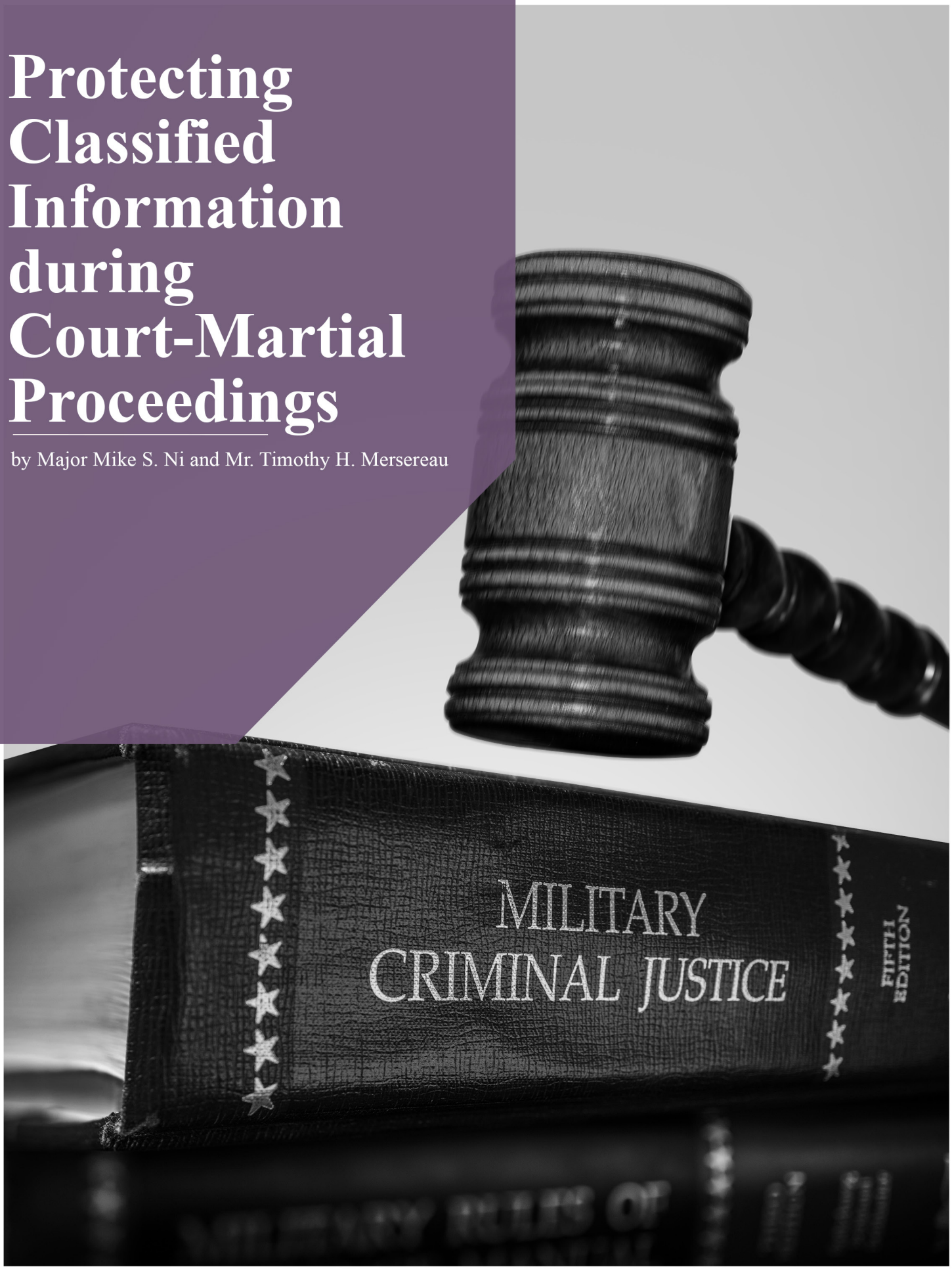
Protecting Classified Information during Court-Martial Proceedings

by Major Mike S. Ni and Mr. Timothy H. Mersereau



United States* v. *Bergdahl

A U.S. Army judge is considering how to handle thousands of documents, many of them classified, that will be part of the case against a soldier who walked off an outpost in Afghanistan.

—CBS News, January 12, 2016

Lawyers for U.S. Army Sergeant Bowe Bergdahl…should have access to classified material to prepare his defense, a military appeals court has ruled….His defense asked for access to 300,000 pages of classified documents and on Feb. 2 a military judge ruled that the defense should have access to all classified information that the government may offer into evidence at trial. The U.S. government appealed the ruling saying the judge had abused his discretion….The Army Court of Criminal Appeals said in its ruling that the military judge had not granted the defense unfettered access to classified information, but only to material in the context of trial discovery.

—Reuters, May 1, 2016

Introduction

On 30 June 2009, United States Army SGT Robert B. Bergdahl walked away from his observation post in Paktika Province, Afghanistan. He was subsequently captured by the Taliban and held until his release on 31 May 2014.[1] What followed was a near 2-year court-martial in which SGT Bergdahl pled guilty to desertion with intent to shirk hazardous duty and misbehavior before the enemy. These were violations of Uniform Code of Military Justice Article 85, *Desertion*, and Article 99, *Misbehavior before the Enemy*.

Evidence in court hearings revealed that thousands of Soldiers, Sailors, Airmen, and Marines conducted an intensive 45-day search for SGT Bergdahl, which resulted in numerous U.S. casualties. Included in such evidence was a substantial amount of classified national security information (or classified information) which, if disclosed to the public, would reasonably cause serious or grave damage to our national security.

United States v. *Bergdahl* is just one example of the complexities of introducing classified information in the courtroom. The intent of this article is to assist military intelligence and security professionals in understanding and navigating the processes of disclosing, and especially protecting, classified information in court-martial proceedings. The article will describe court rules regarding classified information and will identify the roles of notable individuals in the court-martial process, including those with the authorization to determine disclosure.

> “Under no circumstances may a military judge order the release of classified information to any person not authorized to receive such information.”

Overview of Military Rule of Evidence 505

Military Rule of Evidence 505 in the *Manual for Courts-Martial United States* is the primary reference concerning classified information in a military trial. It states, “Classified information must be protected from disclosure if disclosure would be detrimental to national security. Under no circumstances may a military judge order the release of classified information to any person not authorized to receive such information.”[2] As such, people involved in a court-martial cannot request a waiver of Department of Defense rules that protect classified information. If these rules conflict with the rights of the defendant, the protection of classified information takes precedence. Neither the defense counsel nor the government prosecutors have the authority to disclose. Only the head of the executive or military department or government agency that produced the information can authorize the disclosure of classified information.[3]

Key Personnel in Protecting Classified Information in the Court-Martial Process

The following personnel are responsible for protecting classified information in the court-martial process:

- Article 32 hearing officer.
- Military judge.
- Government counsel.
- Defense counsel.
- Security managers.
- Court reporter.
- Sensitive compartmented information (SCI) program manager.
- Bailiffs and military police.

Article 32 Hearing Officer. When significant offenses are alleged against a Soldier, the court-martial process likely begins at an Article 32 preliminary hearing, which determines whether sufficient information exists to support the allegations for the government to proceed to a general court-martial.[4]

Military Judge. Following preferral of charges (i.e., when a Soldier is officially charged with a crime), the case is assigned to a military judge. Everyone in the courtroom can address the military judge as "sir" or "ma'am," consistent with traditional military courtesy, or as "Your Honor." As the head of the court proceedings, the military judge has the additional burden of ensuring that everyone involved upholds the responsibility of all military personnel to protect classified information.

Government Counsel. Government counsel, equivalent to prosecutors, consists of judge advocates from the Office of the Staff Judge Advocate servicing the court-martial convening authority, normally a commanding general. In addition to prosecuting the case, the government counsel is responsible for most administrative matters to bring the case to trial. This includes ensuring proper procedures are in place to present classified information consistent with AR 380-5, *Army Information Security Program*.

Defense Counsel. The defense counsel includes judge advocates from the Trial Defense Service and, at the defendant's expense, may include civilian counsel. Like the government counsel, the defense counsel also must adhere to all rules for accessing classified information and presenting classified evidence.

Security Managers. If it is likely that the court-martial process will involve classified information, the convening authority appoints three security managers—one to advise the military judge, one for the government counsel, and one for defense counsel. Security managers should be an integral part of their respective groups; however, the security managers' sole function is to protect classified information, not to give advice or participate in the trial's strategy in any way. The security managers will work together when necessary to protect classified information; however, they must never exchange any trial tactics, strategy, or other information they have observed about the case. To protect classified information, it is essential that security managers earn the trust of those they advise. This includes counsels' trust that security managers will not share any information that could harm the case in any way.

- ✦ Security managers ensure that everyone they advise has the correct security clearance to view needed classified information. Security managers may assist in obtaining the proper clearance and indoctrinations by coordinating with the appropriate personnel security manager or special security officer.
- ✦ Security managers should assist in obtaining access badges needed to enter the facilities where the relevant classified information is stored.

Glossary of Military Courtroom Terms

Article 32 Hearing. This is the Uniform Code of Military Justice equivalent of a grand jury. In the Article 32 hearing, the government makes its case on whether there should be a trial. The hearing officer of the Article 32 is not a judge. After listening to both sides of the argument, the hearing officer makes a recommendation to the convening authority on the type of court martial, if any.

Article 39A Hearing. Article 39A hearings are procedural hearings that occur before the trial in order to prepare for it. Among many other purposes, parties may agree how they will provide classified information to the defense or how they will present it in the trial.

Government Claim of Privilege. Government agencies are not required to release their classified information to the defense. They can withhold it if they deem it essential to protecting national security information.

Ex Parte Discussion. Typically, if the judge communicates with one side, he must include the other side in the communication. In limited instances, the judge may talk with one side without the other's knowledge. For example, if the government team notifies the court that an agency has claimed privilege (not to allow use of its classified information), that conversation should occur without the defense's knowledge in an ex parte discussion.

In Camera Review. In Latin, *in camera* means "in a chamber." When the judge reviews documents in his office (chambers), or in private, without discussion with the government or defense, he is conducting an in camera review.

- ✦ Security managers should coordinate with the appropriate G-6/S-6 personnel to obtain access to the SECRET Internet Protocol Router Network and with the appropriate special security officer for access to the Joint Worldwide Intelligence Communications System.
- ✦ Security managers should coordinate with G-2/S-2 personnel to obtain a workspace for court members to view and analyze classified information. Government counsel may also assist. Security managers will ensure the workspace has the locks, safes, systems, and other features required for the classification level of the documents that court members will view.
- ✦ Although any court member with the proper clearance can obtain a courier card, the security manager should carry the classified information in order to limit the possibility of security violations or incidents.
- ✦ Security managers must be involved in each counsel's process of preparing witnesses for their testimony. They can provide valuable advice to lawyers and witnesses so that they avoid inadvertent disclosure of classified information in an open (unclassified) hearing. Security managers can advise how to keep presentations unclassified when closed classified hearings are not reasonably possible and how to instruct witnesses to ensure they provide relevant information without revealing the classified sources and methods used to obtain the

information. *Such advice should NOT include telling counsel or witnesses to alter their testimony*. For example, the counsel might believe that a military map with detailed overlays is useful to describe the situation of the crime; however, if the overlays contain classified code words, route names, or other sensitive information, then the security manager should suggest ways to describe the situation without mentioning classified details that add nothing substantive to the testimony.

- ✦ Security managers assist the people they advise with reporting and mitigation if a spillage or unauthorized disclosure occurs.

Court Reporter. The court reporter is a key player in the information flow within the courtroom and therefore is exceedingly important to protect classified information. The court reporter will have a second recording apparatus for "red" proceedings (secret) and a third device for "yellow" proceedings (top secret). The court reporter ensures the audio and video feeds to the overflow spectator area are cut before any red or yellow proceedings.

SCI Program Manager. The SCI program manager approves the establishment of a temporary SCI facility (T–SCIF) at the courthouse if it is required.

Bailiffs and Military Police. Bailiffs are usually a member of the defendant's unit and senior in rank to the defendant (but not less than a sergeant first class). Their tasks are to call the court to attention, obtain witnesses when called to testify, attend to administrative errands during the trial, and maintain the general decorum of the courtroom.[5] Bailiffs are critical to managing access to the courtroom or the T–SCIF and must therefore have a security clearance that matches the classification of the information being presented. Bailiffs do not need to be in the courtroom during the presentation of classified information; instead, they should remain immediately outside the courtroom door to control access. The role of military police is to secure the outer perimeter of the court area and control access to the proceedings, if necessary.

Application of the Military Rule of Evidence 505

Military Rule of Evidence 505 is the government counsel's responsibility to contact any or all government agencies that may have information relevant to the case. The government counsel must segregate classified information and review it for relevancy. All government agencies are obligated to provide their information; however, they are not obligated to allow the information to be used in court or shown to the defense. When dealing with classified information originating from outside the Army, those individuals involved in the case must remember that merely having the appropriate security clearance does not give anyone carte blanche to see all the classified products, even if the products are relevant to the case.

The government counsel also has the responsibility to provide evidence to the defense. The defense counsel normally has access to any or all information relevant to the case to best represent their client and to ensure that due process is upheld. Before the release of information to the defense, Military Rule of Evidence 505 requires that the government review all classified information pertaining to the case to determine *only that information which directly applies* before its release to the defense counsel. The government counsel reports to the military judge what will not be released. While the defense counsel may not always agree with the government's decision to withhold certain classified information, it is essential to preserve the need-to-know principle of information security.

A gavel rests on the judge's bench in the courtroom of the 39th Air Base Wing legal office, November 14, 2019, at Incirlik Air Base, Turkey. The defendant was being tried for sexual assault. The verdict was not guilty[6] (U.S. Air Force photo by SSgt. Joshua Magbanua)

The release authority is the head of the executive or military department of the government agency concerned. This applies to the "right of originator to refuse presentation." The originator decides whether to allow the release of its classified information to the defense counsel or to allow its use in court. The originator might decide not to release the information at all. The originator makes its decision based on national security and is not required to defend its position. The originator's privilege is the "government claim of privilege." If an originator invokes the privilege, the government must notify the military judge. If the originator does not want the public or the defense counsel to know about its claim of privilege, the government does not have permission to notify them.

When invoking government claim of privilege, the originator may still allow the court to use a written summary of the classified information. For example, imagine the government counsel identified a top secret document produced by the Central Intelligence Agency (CIA). The CIA may preclude the document's release because it will reveal sources and methods to those with no need-to-know. The CIA and government counsel may collaborate to provide a secret document summarizing only those parts relevant to the case. Before the defense counsel receives the document, the military judge reviews the original document and the summary to ensure they only include relevant information.

It is also important for the government counsel to build and use a roster to track who has access to classified information in the court-martial process. This roster is useful to control entry in classified court proceedings.

Open and Classified Hearings

The general principle is for both the government and the defense to strive to make the hearings unclassified and accessible (open) to the public. Closed hearings should occur only when there is no alternative because of the need to present classified information. There are three types of hearings: open, secret, and top secret and SCI.

Open Hearings. An open hearing occurs at the unclassified level and is open to the public and the press. The court may provide overflow viewing areas, if necessary. During these hearings, security managers should sit in a place where they are readily accessible to those they support, i.e., military judge, government counsel, and defense counsel.

Secret Hearings. A secret hearing, also known as a "red" or collateral hearing, occurs after security managers have ensured the facility is adequate for secret discussions. If the hearing "goes red," it is necessary to cut all transmissions, such as the audio feed to the spectator overflow room. The court reporter should only record on a recording device authorized for secret information. Essential personnel identified ahead of time may remain present. Bailiffs will escort all nonessential personnel from the courtroom. For this type of hearing, the court should not provide overflow viewing areas in the event someone inadvertently leaves the audio or video feeds turned on. During the classified proceeding, bailiffs should stand outside the courtroom door and control all access, such as the calling of witnesses. These restrictions disrupt the transparency and flow of the proceeding; therefore, the use of secret hearings should be minimal and planned for ahead of time.

Top Secret and SCI Hearings. Hearings for top secret information and for SCI, known as "yellow," have similar procedures. (In some instances, the SCI information may have a classification lower than top secret.) However, courtrooms are rarely adequate to serve as a T–SCIF. Before the trial, the SCI program manager should work with the government counsel to identify an available T–SCIF. Again, it is important to identify authorized participants ahead of time and record their names on an access roster. Before the trial, it also important to ensure the lawyers and other court members have the relevant security clearances. In some instances, individuals may need to be "read on" for specific SCI programs. However, there will likely not be time to clear panel members (aka, jurors). Therefore, in addition to maintaining a fair and impartial panel, security clearances are an important consideration when selecting panel members if either side intends to introduce top secret information and/or SCI.

Best Practices

The primary best practices to protect classified information during a court-martial are—

- Rehearse.
- Be prepared to establish a T–SCIF.
- Prepare for inadvertent disclosure in an open hearing.

Rehearse. It is essential to practice the procedures for presenting classified information ahead of time, including a rehearsal for both "red" and "yellow" procedures. Key members of government and defense counsels, security managers, court reporter, bailiffs, and military police should all be present.

Be Prepared to Establish a T–SCIF. If it is not feasible to hold the hearing in an existing SCIF, it may be beneficial to establish a T–SCIF at or near the courthouse.

Prepare for Inadvertent Disclosure in an Open Hearing. If someone inadvertently divulges classified information in an open hearing, security managers should have a mechanism to notify their respective teams with a visual but discreet signal. We must be discreet so that we do not draw attention from the public and the press, indicating to them that they may have just heard sensitive information; this is part of the mitigation. When the military judge receives the signal, they should stop the proceeding, call a recess, permit the security managers to explain what occurred, and convert to a closed classified hearing, if necessary. The incident report should identify the unauthorized disclosure through normal reporting channels.

Conclusion

With our conditioning as military intelligence and security professionals, we are often quick to say, "You can't do that," or in the case of courts-martial, "You can't discuss classified testimony outside the SCIF." However, with the application of expert knowledge and some creativity, you can establish a secure environment for virtually any testimony. The real art of security is when we combine imagination with our extensive knowledge of the regulations. In our daily work, this

approach allows us to accomplish the operational mission without compromising security. In the courtroom, we have an inherent responsibility to national security to ensure everyone presents classified evidence securely and appropriately.

American jurisprudence requires a transparent justice system. However, it must maintain a balance between ensuring a defendant's due process and protecting national security by not allowing the unauthorized disclosure of classified information. *United States* v. *Bergdahl* is a prime example of the defense counsel seeking thousands of pages of classified documents, arguing that they were necessary to satisfactorily defend their client and ultimately obtain a fair trial. While not every case may be as high profile as the Bergdahl case, scrutiny and caution are paramount when classified information is present.

Epigraph

"Classified documents prompt debate in Bowe Bergdahl case," CBS News, January 12, 2016, https://www.cbsnews.com/news/bowe-bergdahl-case-classified-documents-prompt-debate/.

"Bergdahl defense can access classified information, court rules," Reuters, May 1, 2016, https://www.reuters.com/article/uk-usa-defense-bergdahl-idUKKCN0XS1I9.

Endnotes

1. *United States* v. *Bergdahl*, No. 19-0406 (C.A.A.F. 27 August 2020).

2. Joint Service Committee on Military Justice, *Manual for Courts-Martial United States* (Washington, DC, 2019), III-24.

3. Ibid., III-24–III-29.

4. Article 32, Uniform Code of Military Justice, and Rule for Courts-Martial 405.

5. Rule for Courts-Martial 501(c) and U.S. Army Trial Judiciary, *Rules of Practice before Army Courts-Martial* (1 January 2019), 24, 30–31.

6. SSgt Joshua Magbanua, "Back in session: courts-martial return to Incirlik," Incirlik Air Base website, November 15, 2019, https://www.incirlik.af.mil/News/Article-Display/Article/2017423/back-in-session-courts-martial-return-to-incirlik/.

References

Department of Defense (DoD). DoD Manual 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*. Washington, DC, February 24, 2012, incorporating change 2, July 28, 2020.

Department of the Army. Army Regulation (AR) 380-5, *Army Information Security Program*. Washington, DC: U.S. Government Publishing Office (GPO), 22 October 2019.

Department of the Army. AR 380-28, *Army Sensitive Compartmented Information Security Program*. Washington, DC: U.S. GPO, 13 August 2018.

MAJ Mike Ni is an administrative law attorney in the Office of the Staff Judge Advocate for the U.S. Army Intelligence and Security Command (INSCOM).

Mr. Tim Mersereau is the Deputy G-2 at INSCOM, and he served as security advisor to the judge during the court-martial hearings and trial of the United States *v.* Bergdahl.