ATP 3-16.02

WRITE FOR RELEASE

SEPTEMBER 2023

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

HEADQUARTERS, DEPARTMENT OF THE ARMY

This publication is available at the Army Publishing Directorate site (https://armypubs.army.mil/) and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard).

Army Techniques Publication
No. 3-16.02

Headquarters
Department of the Army
Washington, D.C., 26 September 2023

WRITE FOR RELEASE

Contents

Figures

Tables

Vignettes

This page intentionally left blank.

Preface

ATP 3-16.02 provides fundamental principles and guidance for Army forces who operate as part of a multinational operation or coalition to produce information products that will be released to our partners. It will blend key points regarding writing documents and producing products for release and its approach to ensure consideration by Army elements of a joint force and addresses the Army expeditionary staff roles and functions in a multinational operation that contribute to unified action. This publication provides guidelines and practical examples to achieve an information-sharing culture. It can assist a multinational commander to understand and develop solutions to build an effective fighting force with the ability to share critical information to minimize the foreign disclosure officer review process.

The audience for ATP 3-16.02 is all Army professionals. Commanders and staff members of U.S. Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces.

Commanders and staffs ensure that disclosure decisions follow National, Department of Defense, and Army disclosure policies. Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States, international, and in some cases, host-nation laws and regulations when applying this doctrine. Commanders at all levels ensure their Soldiers operate in accordance with the law of armed conflict and the rules of engagement as discussed in FM 6-27.

ATP 3-16.02 uses joint terms where applicable. Selected joint and U.S. Army terms and definitions appear in both the glossary and the text. There are no terms or definitions for which ATP 3-16.02 is the proponent publication. When first defining other proponent definitions in the text, the term is italicized, and the number of the proponent publication follows the definition.

ATP 3-16.02 applies to the Active Army, the Army National Guard/Army National Guard of the United States, and United States Army Reserve unless otherwise stated.

The proponent of ATP 3-16.02 is the United States Army Combined Arms Center. The preparing agency is the Mission Command Center of Excellence, United States Army Combined Arms Center. Send comments and recommendations on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, United States Army Combined Arms Center and Fort Leavenworth, ATZL-MCD (ATP 3-16.02), 300 McPherson Avenue, Fort Leavenworth, KS 66027-1300; by email to usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@army.mil; or submit an electronic DA Form 2028.

Introduction

To enable effective information sharing in future multinational operations and exercises, it is imperative that authors and other originators of classified information understand and apply the precepts of ATP 3-16.02, *Write for Release*.

Write for release is a deliberate process of producing information with the intent and knowledge that Soldiers may disclose the final product to unified action partners. Write for release is also a major culture shift for authors and other originators of classified information, requiring deliberate planning of their content to meet information-sharing and releasability requirements for the target audience. The write for release process guides all staff members through writing products with the intent to share with mission partners. This differs from the after-production, tear-line method of sharing information. The write for release process speeds up disclosure emphasizing proactive pre-production disclosure decisions versus reactive post-production disclosure decisions. Legacy information systems, processes, and product development focus on information security, with minimal regard for sharing information outside the Army.

Write for release, the balancing of information security and information sharing, is important today and in the future. FM 3-0's operational concept and multidomain operations highlight the requirement for interoperability. An Army formation that is interoperable with joint and multinational partners is substantially more capable than one that is not interoperable. Interoperability with any unified action partner is essential to effective operations. Interoperability standards and procedures must be trained, tested, and refined during competition; it is too late to seek interoperability once a crisis or armed conflict begins. One key to effective interoperability is the ability to share information among mission partners—partners with which the Department of Defense (DOD) cooperates to achieve national goals. The write for release process enables increased information sharing with mission partners without sacrificing information security, avoiding over-classification and improper portion marking through deliberate analysis of what information must be shared. The write for release process also describes how to share information in accordance with all published security classification guides and other constraints and limitations.

ATP 3-16.02 contains ten chapters and three appendixes:

Chapter 1 discusses how the write for release (WFR) process fits into the mission partner environment, the framework of human, procedural, and technical domains to achieve desired levels of interoperability with mission partners in an exercise or operation.

Chapter 2 identifies categories of military information and describes commander and staff responsibilities with respect to the WFR process.

Chapter 3 discusses the external factors—constraints and limitations—authors and other originators consider when conducting the WFR process.

Chapter 4 provides an overview of the WFR process. It summarizes each of the five steps in the process.

Chapter 5 discusses the first step in the WFR process, requirements determination. This step uses research to determine the information sharing requirements and the associated risks, constraints, and limitations.

Chapter 6 discusses the second step in the WFR process, requirements analysis. This step implements analysis and evaluation of the information sharing requirements against the associated risks, constraints, and limitations to develop information sharing courses of action.

Chapter 7 discusses the third step in the WFR process, pre-production. This step involves gathering the tools to ensure released products comply with disclosure authorities.

Chapter 8 discusses the fourth step in the WFR process, production. This step focuses on timely and accurate document marking, change management, and mapping of the intended means of disclosure, distribution, or both.

Chapter 9 discusses the fifth and final step in the WFR process, disclosure and dissemination. This step uses actions and activities required to securely share required information with mission partners.

Chapter 10 identifies the assessment considerations in each step of the WFR process. It addresses sample measures of performance and measures of effectiveness as well as a sample checklist as an aid to assessment.

Appendix A lists references by category that support this publication.

Appendix B provides a potential checklist for the commander and staff to aid in implementing the WFR process.

Appendix C provides examples for troubleshooting incorrect banning of shared information that can hinder the WFR process.

Chapter 1

Write for Release and the Mission Partner Environment

This chapter introduces the write for release (WFR) process to the Army and addresses benefits of writing for release within the mission partner environment (MPE). First, the chapter gives an overview of the WFR process. Then it briefly discusses benefits of the WFR process. It concludes with a brief overview of an MPE and description of the WFR process with the interoperability domains.

INTRODUCTION TO THE WRITE FOR RELEASE PROCESS

1-1. The WFR process is a new way of thinking for the Army. For information sharing, the Army has used *write to protect* rather than *write for release*. As the Army becomes more accustomed to operating with unified action partners, it is imperative that WFR becomes common practice for effective information sharing. The write for release process is a deliberate and continuous organizational process for producing information with the intent and foreknowledge that the final product may be disclosed to mission partners.

> ***Note.*** This publication uses *unified action partner* and *mission partner*. They have different meanings. AR 34-1 describes unified action partner as Joint Forces, multinational partners, and interagency and nongovernmental organizations. DODD 5101.22E describes a mission partner as any partner not in the United States military or Department of Defense.
>
> The terms are not interchangeable. A mission partner is always a unified action partner; however, a unified action partner is not always a mission partner.

1-2. The WFR process begins with the intention of sharing information, is essential to achieving information advantage, and anticipates that all information is subject to sharing with mission partners. The WFR process is a five-step, requirements-driven process that can start, stop, skip, and restart as the mission and receipt of information dictates. The WFR process is an organizational process used to create, write, produce, and disseminate all information within an MPE. This process involves and affects any partners operating in the MPE. The WFR process belongs to the commander. A successful process requires the entire staff to understand and operate within the commander's intent for information sharing.

1-3. The five steps of the WFR process are—

- Requirements determination.
- Requirements analysis.
- Pre-production.
- Production.
- Disclosure and dissemination.

Figure 1-1 shows the five steps of the WFR process and how the process touches each of the three interoperability domains. Later chapters discuss each of the five steps in greater detail.

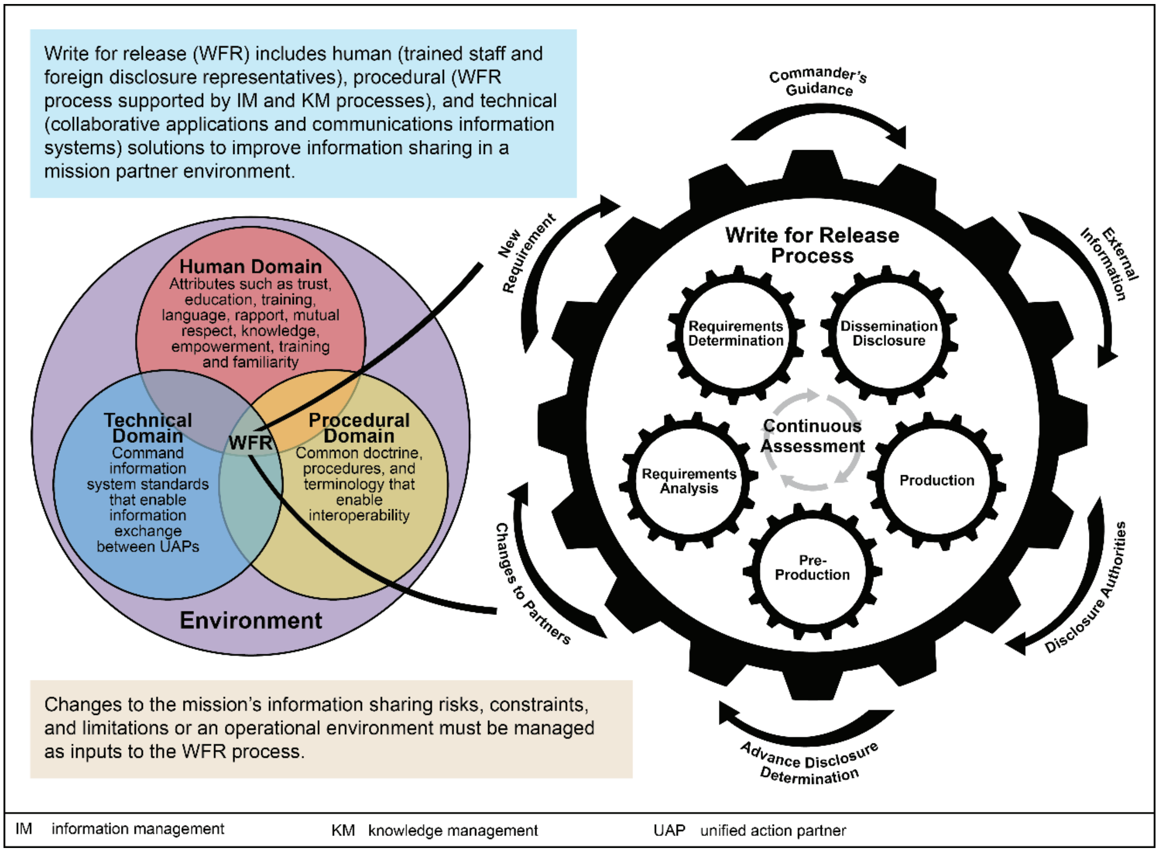

Figure 1-1. Five-step write for release

BENEFITS OF THE WRITE FOR RELEASE PROCESS

1-4. When operating with mission partners, WFR is critical to overall mission success. The WFR process has four benefits as it relates to an MPE:

- Shared understanding.
- Speed.
- Adaptable.
- Achievable.

SHARED UNDERSTANDING

1-5. The first benefit for Army forces using WFR is a shared understanding. Achieving shared understanding is critical within an MPE. The WFR process supports an environment for information sharing, which improves the coordination and communication among all partners. Achieving shared understanding requires staffs to write information allowing for the widest distribution possible. (Refer to FM 3-16 and ABCANZ Publication 332 for more information on operations with mission partners.)

SPEED

1-6. When operating in an MPE, speed is another benefit accomplished with WFR. Soldiers save time using all five of the WFR process steps by determining what and with whom they will share information. Additionally, the WFR process increases the speed of the sharing of information by alleviating the need for a complete or full release determination by the foreign disclosure officer.

ADAPTABLE

1-7. Another benefit for the Army with using WFR is adaptability. The WFR process is not a linear process. Instead, the process is driven by information sharing requirements. Adaptability specifically benefits an MPE because changes occur regularly. Such changes can include flux in policy or agreements, commander's intent or guidance, and the addition or removal of partners. Changes do not stop operations or prevent units from conducting the process.

ACHIEVABLE

1-8. When operating in an MPE, achievability is another benefit with WFR. Soldiers can execute the WFR process at any level from national to tactical. Achievable information sharing occurs when Soldiers follow information sharing agreements, security classification guides (SCGs), policies, and commander's intent or guidance.

THE MISSION PARTNER ENVIRONMENT OVERVIEW

1-9. An MPE is an operating framework enabling command and control and information sharing for planning and execution across the full range of military operations at a single security level with a common language. An effective MPE includes technical, human, and procedural domains of interoperability to enable timely, complete, and accurate information sharing and unity of effort among mission partners. The three interoperability domains, human, procedural and technical, directly apply to the MPE framework. These domains are discussed in paragraphs 1-10 through 1-12.

> ***Note.*** Operational environment is the fourth attribute of the MPE. As shown in Figure 1-1, the domains are part of the MPE; they are not operational dimensions.

HUMAN

1-10. When applied to the WFR process, the human domain is a foundational maxim for the process. All partners operating in an MPE decide what information to share. They base their decisions on policy, sharing agreements, and commander's intent or guidance. Once partners identify information to share, units conduct the WFR process to ensure information is shareable.

PROCEDURAL

1-11. The WFR process facilitates information sharing across an MPE. The WFR process improves the Army forces' ability to share information among partners in a timely manner. Additional characteristics that partners consider in an MPE can include common doctrine, standard operating procedures, knowledge management, bilateral or multilateral agreements, and commander's intent or guidance.

TECHNICAL

1-12. For the purposes of the WFR process, the technical domain in mission command systems includes a mission partner network (MPN). The MPN is the network portion of the MPE. It is a specific partnership or coalition wide area network planned and implemented using standards and protocols agreed to by the participants. The MPN uses operational and theater strategic enterprise transport assets that facilitate the sharing of information using common protocols and standards among those mission partners operating on it.

This page intentionally left blank.

Chapter 2
Responsibilities

This chapter provides an overview of the categories of military information and the responsibilities of select staff sections within the WFR process. The chapter first introduces the categories of military information. The chapter then briefly describes the responsibilities for all staff sections within the WFR process. The chapter concludes with a brief description of the responsibilities of select staff sections.

CATEGORIES OF MILITARY INFORMATION

2-1. Delegated disclosure authorities are policies written at the national level that identify the maximum classification levels in each category of military information that the Army may disclose to foreign governments or international organizations. These delegated disclosure authorities are based on the partner, classification, and category of information. Knowing the categories of information enables commanders and staffs to determine which delegated disclosure authority to use when operating within an MPE. (Refer to the *National Disclosure Policy*-1 for more on delegated disclosure authorities.)

2-2. U.S. staffs must understand the categories of military information to facilitate planning, execution, and assessment of the WFR process. This understanding allows for the timely and relevant sharing of information. Table 2-1 describes the eight categories of military information. See Appendix A for a more detailed discussion and examples of each category.

Table 2-1. Categories of military information

Category	***Description***
Category 1: Organization, Training, and Employment of Military Forces	Includes military information of a general nature; organization of military, paramilitary, or irregular forces, and TTP used to train and employ those forces
Category 2: Military Materiel and Munitions	Includes all military materiel, arms, and munitions procured or controlled, adopted, produced, or used by the Department of Defense
Category 3: Applied Research and Development Information and Materiel	Involves the element of time within engineering data, general operational requirements, concepts, and military characteristics required to adopt items for production
Category 4: Production Information	Relates to designs, specifications, manufacturing techniques, and information necessary to manufacture materiel and munitions
Category 5: Combined Military Operations, Planning, and Readiness	Does not include strategic plans and guidance or North American defense information as North American defense information is its own category.
Category 6: Order of Battle	Includes the identification, strength, command structure, and disposition of personnel, units, and equipment located in a territory under the jurisdiction of the recipient government (host partner nation) or otherwise direct concern
Category 7: North American Defense	Relates to the plans, operations, programs, and projects, to include data and equipment, directly related to North American defense
Category 8: Military Intelligence	Includes information of a military character and pertains to foreign nations. This category is about foreign nation information and not about U.S. Army intelligence
Legend: TTP tactics, techniques, and procedures U.S. United States	

STAFF RESPONSIBILITIES

2-3. All staff members have a responsibility during the WFR process as they manage information related to their individual areas of expertise. Paragraphs 2-4 through 2-17 discuss only select staff sections that have more prominent information sharing roles. (Refer to FM 6-0 for a full description of roles and responsibilities of all staff sections.) All staff members, as recipients and distributors of information, must be knowledgeable in the categories of military information. While specific staff sections may execute the WFR processes more frequently or for larger quantities of information, all staff sections remain prepared to conduct the WFR process as the military information pertains to their functional areas. All staff sections participate in the WFR process.

ALL STAFF ELEMENTS WRITE FOR RELEASE RESPONSIBILITIES

2-4. Regardless of the mission or method of communications, during the WFR process, all staff sections share these common responsibilities:

- Identify and resource staff section needs or requirements for foreign disclosure representatives.
- Identify information sharing requirements.
- Identify requirements for sharing external mission-critical information with partners.
- Provide guidance to the staff on the requirements, formats and markings, and prohibitions for disseminating information to partners through the various command and control systems.
- Write all annexes, orders, and documents with the intent to share with mission partners for all communication (oral, visual, or documentary) methods.
- Initiate all products on the MPN as applicable.

THE COMMANDER

2-5. The commander provides the overall guidance and direction to the organization for mission accomplishment. The commander's primary responsibilities in the WFR process:

- Establish and maintain a climate of sharing information with partners. Communicate commander's intent for information sharing with mission partners.
- Formally appoint the required number of foreign disclosure officers to support the staff in an MPE.
- Understand and ensure staff application of all categories of military information.

When providing guidance, commanders ask many questions to their organizations and staff. See Appendix B for potential questions that commanders use to identify their information sharing requirements.

THE CHIEF OF STAFF OR EXECUTIVE OFFICER

2-6. The chief of staff or executive officer is the commander's principal staff officer and the key staff integrator. During the WFR process, the chief of staff or executive officer responsibilities include—

- Coordinating and directing the work of the staff, including the foreign disclosure officers.
- Establishing, monitoring, and synchronizing the WFR process across the staff.
- Enforcing guidance and administrative standards necessary for the WFR process across the staff, particularly those written with or agreed upon between partners.
- Providing oversight for implementing bilateral and multilateral information sharing agreements.
- Understanding and ensuring the staff applies the categories of military information.

G-1 OR S-1, PERSONNEL

2-7. The G-1 or S-1 is the principal staff officer for all matters concerning human resources, both military and civilian. During the WFR process, the G-1 or S-1 responsibilities—

- Provide subject matter expertise and recommendations for sharing Category 1 (Organization, Training, and Employment of Military Forces) and Category 5 (Combined Military Operations, Planning, and Readiness) information.

- Identify Category 1 and Category 5 information sharing requirements.
- Coordinate within an MPE for authority to share Category 1 and Category 5 information. This includes information and products obtained from partners.

G-2 or S-2, Intelligence

2-8. The G-2 or S-2 is the chief of the intelligence warfighting function and the principal staff officer responsible for providing intelligence to support current and future operations and plans. Category 8 is about foreign nation information and not about U.S. Army intelligence. During the WFR process—

- The G-2 or S-2 provides subject matter expertise and recommendations for sharing Category 8 (Military Intelligence) information.
- The G-2 or S-2 identifies Category 8 information sharing requirements.
- The G-2 or S-2 coordinates for authority to share Category 8 information. This includes information and intelligence products obtained from partners.
- The G-2 or S-2 ensures the staff understands and adheres to specific or unique guidance related to sharing Category 8 information.
- The S-2 trains the staff in marking of documents as part of their information security mission.

G-3 or S-3, Operations

2-9. The G-3 or S-3 is the chief of the movement and maneuver warfighting function and the commander's principal staff officer for coordinating and synchronizing all operations in their entirety. During the WFR process, the G-3 or S-3 responsibilities are the following:

- Provide subject matter expertise and recommendations for sharing Category 1 (Organization, Training, and Employment of Military Forces), Category 5 (Combined Military Operations, Planning, and Readiness), Category 6 (Order of Battle), and when necessary Category 7 (North American Defense) information.
- Identify Category 1, Category 5, Category 6, and Category 7 information sharing requirements.
- Coordinate for authority to share Category 1, Category 5, Category 6, and Category 7 information.

G-4 or S-4, Logistics

2-10. The G-4 or S-4 is the chief of the sustainment warfighting function and the principal staff officer for sustainment plans and operations, supply, maintenance, transportation, and services. During the WFR process, the G-4 or S-4 responsibilities are—

- Providing subject matter expertise and recommendations for sharing Category 2 (Military Materiel and Munitions) information.
- Identifying Category 2 information sharing requirements.
- Coordinating for authority to share Category 2 information.

G-5 or S-5, Plans

2-11. The G-5 or S-5 is the principal staff officer for planning operations for the mid- to long-range planning horizons. The plans officer leads the staff in preparing plans and orders to meet the commander's guidance. The responsibilities of the G-5 or S-5 during the WFR process are the following:

- Conduct mission analysis in an MPE with mission partners during the U.S. military decision-making process while using the WFR process to guide classifications and disclosure of plans to partners.
- Provide subject matter expertise and recommendations for sharing Category 1 (Organization, Training, and Employment of Military Forces), Category 5 (Combined Military Operations, Planning, and Readiness), Category 6 (Order of Battle), and when necessary, Category 7 (North American Defense) information.
- Identify Category 1, Category 5, Category 6, and Category 7 information sharing requirements.
- Coordinate for authority to share Category 1, Category 5, Category 6, and Category 7 information.

G-6 or S-6, Signal

2-12. The G-6 or S-6 is the principal staff officer responsible for all matters concerning communications within the unit's area of operations. The signal officer's responsibilities include network operations and applicable portions of defensive cyberspace operations, network transport, information services, spectrum management operations, and information management. During the information management process of writing for release, the G-6 or S-6 responsibilities are—

- Establishing and maintaining both the unit network and the MPN.
- Establishing standard instructions for joining, membership, and exiting instructions (known as JMEI) from the MPN.
- Determining supportability, feasibility, and disclosure requirements of signal plans using the WFR process.

G-9 or S-9, Civil Affairs Operations

2-13. The G-9 or S-9 is the principal staff officer at echelons brigade and above responsible for all matters concerning civil affairs and civil-military operations. During the WFR process, the G-9 or S-9 responsibilities are the following:

- Provide subject matter expertise and recommendations for sharing Category 1 (Organization, Training, and Employment of Military Forces), Category 5 (Combined Military Operations, Planning, and Readiness), and Category 6 (Order of Battle).
- Identify Category 1, Category 5, and Category 6 information sharing requirements.
- Coordinate for authority to share Category 1, Category 5, and Category 6 information.
- Provide subject matter expertise and oversight for sharing all civil affairs information.

The Foreign Disclosure Officer

2-14. The foreign disclosure officer is appointed by the commander. In coordination with the chief of staff or executive officer, the foreign disclosure officer oversees and coordinates the disclosure of categories of military information or controlled unclassified information (CUI) to representatives of foreign governments and international organizations. During the WFR process, the foreign disclosure officer responsibilities are—

- When authorized, make disclosure decisions for the commander.
- Inform and advise the commander and staff on the current delegated disclosure authorities by country, category of information, and classification level.
- Advise the commander on the recommended number and location of foreign disclosure representatives based on mission requirements.
- Train foreign disclosure representatives on disclosure authorities and responsibilities.
- Direct the information production requirement efforts (write for release) in the organization for all categories of classified military information and CUI to ensure adequate disclosure to partners.
- Lead coordination efforts for the authority and permission to disclose information originated outside the organization.
- Develop and publish foreign disclosure guidance for deployments, exercises, training events, and official foreign visits and visitors (including exchange and liaison officers).
- Prepare the commander for engagements with multinational and mission partners from a foreign disclosure perspective.
- Adhere to the *National Disclosure Policy-1* provisions for false impressions.

Public Affairs Officer

2-15. The public affairs officer coordinates and synchronizes themes and messages as addressed in FM 6-0. During the WFR process, the public affairs officer responsibilities are—

- Coordinate with the security manager and the foreign disclosure officer as required.
- Gain approval from partners for public disclosure of foreign government information.
- Coordinate with the foreign disclosure officer for the release of any visual information as required (for example, combat camera).

The Provost Marshal

2-16. The provost marshal is the senior military police officer and is responsible for assisting the commander in exercising control over military police forces in the area of operations. During the WFR process, the provost marshal's responsibilities are to coordinate the sharing of law enforcement sensitive and force protection information.

Liaison Officer

2-17. A liaison officer is an individual who represents the commander or staff officer to maintain contact or intercommunication between units or organization. During the WFR process, liaison officer responsibilities include the following:

- Adhering to the *National Disclosure Policy*-1 provisions for false impressions.
- Obtaining and conveying information requirements back to their sending unit headquarters.
- Assisting the sending unit in coordinating the disclosure of information originating with receiving unit partners. Permission is required to share partner information.

Surgeon

2-18. The surgeon is a Medical Corps officer and member of the commander's personal and special staff. The surgeon advises the commander and the staffs on all medical or medical-related issues. The surgeon is responsible for coordinating health assets and operations within the command. This officer provides and oversees medical care to Soldiers, civilians, and detainees. During the WFR process, the surgeon's responsibilities are to advise the commander and their staff on all medical or medical-related issues. (Refer to FM 4-02 for more information on the role of the surgeon and surgeon section at echelon.)

Operations Security Officer

2-19. The operations security officer is responsible for the development, organization, and administration of the operations security program. During the WFR process, the operations security officer is responsible for providing guidance and direction on sharing information that falls outside the purview of National, DOD, and U.S. Army disclosure policies with foreign personnel.

This page intentionally left blank.

Chapter 3

Understanding External Factors

This chapter discusses the external factors that influence the WFR process. It starts by defining constraints and limitations. It provides a brief overview of how the WFR process is affected, then provides examples. The chapter concludes with a brief overview of planning for these external factors.

EXTERNAL FACTORS: CONSTRAINTS AND LIMITATIONS

3-1. All the dimensions of an MPE are subject to external factors. These external factors are known as constraints and limitations. Commanders and staffs must know, understand, and account for these factors during the planning process.

3-2. A *constraint* is a restriction placed on the command by a higher command. A constraint dictates an action or inaction, thus restricting the freedom of action of a subordinate commander (FM 5-0). Constraints are identified during mission analysis of the military decision-making process and will influence the commander's decision making throughout an entire operation. Examples of constraints related to WFR include information sharing agreements, SCGs, policies, laws, and higher commander's guidance.

3-3. Limitations are factors or conditions that either typically or permanently impede mission accomplishment. Like constraints, limitations are identified during mission analysis of the military decision-making process. With respect to the WFR process, limitations will change over time. Accordingly, an MPE changes over time along with the information that staffs can share. Examples of WFR limitations include lack of process and procedures, delegated disclosure authorities, and markings or dissemination caveats.

EXAMPLES OF CONSTRAINTS

3-4. Constraints exist in many forms. When using the WFR process, Soldiers often use information sharing agreements and SCGs.

INFORMATION SHARING AGREEMENTS

3-5. Partner nations use information sharing agreements to work together to set up parameters on methods to share information. Adhering to these formal agreements preserves trust among partner nations. These agreements are procedural solutions. Examples of these types of sharing agreements include multilateral and bilateral agreements, national policies, standardization agreements, and delegation of disclosure authorities (Refer to DODI 5530.03 for information on international agreements.)

SECURITY CLASSIFICATION GUIDES

3-6. A SCG communicates an original classification decision by listing a collection of precise decisions and comprehensive guidance regarding a specific system, plan, program, mission, or project by discrete segments of information or data. In other words, a SCG is the original source classification with detailed reasoning for the classification. The SCG provides the reader with the necessary guidance when assigning the appropriate level of classification. At times, the guide provides the reader with a range of possible classification levels, related to specific topics, or segments of information. Aggregated information increases the classification through compilation, and the guide warns readers when necessary.

EXAMPLES OF LIMITATIONS

3-7. Many types of limitations also exist. The WFR process is affected by the following types of limitations: delegated disclosure authorities, markings and dissemination caveats, distribution statements, proponent consent, and MPN.

DELEGATED DISCLOSURE AUTHORITIES

3-8. Required by national and DOD policies, delegated disclosure authorities are policies delegated by country, category of information, and classification level to formally designated individuals by position. Delegated disclosure authorities exist in two forms:

- Standing authority as delineated in Annex A of *National Disclosure Policy*-1.
- Temporary authority as delineated by a national disclosure policy committee decision in the form of a record of action. Records of action are typically the result of an exception to national disclosure policy that establishes limited purpose or limited duration increases to the standing authorities.

MARKINGS AND DISSEMINATION CAVEATS

3-9. Staffs use the WFR process for all markings and dissemination caveats, such as CUI, foreign government information, limited distribution, and law enforcement sensitive. Paragraphs 3-10 through 3-13 discuss only a few examples. For the purposes of security and control, markings and dissemination caveats reflect decisions made by an information proponent. Staffs mark aggregated information with the highest classification contained in a document or collection of information. Paragraph or portion markings represent the highest classification contained in the segment. Dissemination caveats provide formal notice and articulate a warning or proviso of specific stipulations, conditions, or limitations. Common markings and dissemination caveats include the following:

- Not releasable to foreign nationals.
- Originator controlled.
- Releasable by information disclosure official.
- Releasable to.

Not Releasable to Foreign Nationals

3-10. Not releasable to foreign nationals (NOFORN) prohibits release of information to foreign nationals. The U.S. Government has determined that certain select topics and information are so sensitive, or central to internal to the U.S. Government only, that staffs need to readily identify documents as such to ensure their continued protection. Staffs ensure readers know the U.S. Government's deliberate decision to exclude foreign national access to these select topics and information sets with clear markings of NOFORN. This caveat is extremely restrictive, and staffs should only apply it when justified by specific policy. NOFORN is typically reserved for intelligence information and other sensitive topics such as the *National Disclosure Policy*-1. (Refer to Annex A of *National Disclosure Policy*-1 for a discussion of justified and necessary application of the NOFORN caveat.)

Originator Controlled

3-11. The originator controlled (known as ORCON) caveat is placed on classified national security information. This marking indicates that staffs may disseminate the document to other Federal agencies but not outside the executive branch without the prior approval of the originating agency.

Releasable by Information Disclosure Official

3-12. The releasable by information disclosure official (known as RELIDO) caveat reflects the originator's decision that defers the foreign disclosure decision to the senior disclosure and release authority. The staff typically applies the releasable by information disclosure official caveat to products and information originating within the intelligence community.

Releasable To

3-13. The releasable to (known as REL TO) marking indicates that an affirmative disclosure determination has already been made. In this case, the information has already been disclosed or may be disclosed in the future to the country or international organization further delineated in the marking string.

DISTRIBUTION STATEMENTS

3-14. Distribution statements denote the extent of the information’s availability for secondary distribution, release, and disclosure without need for additional approvals or authorizations from the controlling DOD office. (Refer to DODI 5230.24 for a complete list of all distribution statements.)

PROPONENT CONSENT

3-15. Several of the discussed caveats warn of needing proponent consent. The proponent consent is a fundamental aspect of most disclosure policies. For staffs to approve the disclosure of information, a commander must formally authorize them to do so and the proponent must grant permission to do so.

MISSION PARTNER NETWORK

3-16. The MPN can slow the WFR process by limiting the transmission of information from one partner to another. Network architecture, security, and data standards illustrate short-term limitations. However, planners need to consider effects of long-term limitations on the WFR process, such as changes to network operations and emerging technologies on technical interoperability with partners.

PLANNING FOR EXTERNAL FACTORS

3-17. Implementation of the WFR process early during the planning phase is essential when operating with unified action partners. Acknowledgment and mitigation of both constraints and limitations is critical to mission success. As most constraints to the WFR process are external to the organization, early identification and mitigation are critical to ensure successful information sharing.

3-18. Practical examples of external factors are provided so that—

- There is a contextual understanding of the external factors.
- Understanding exists at the beginning of the process, so staffs can plan for external factors and mitigate where possible.
- Staffs realize and acknowledge that these external factors require organizational awareness and attention as they extend beyond the realm of the intelligence and security communities.

3-19. The vignettes on pages 3-4 and 3-5 present real-life scenarios that staffs may encounter. After each vignette, paragraphs 3-20 through 3-22 each discuss the decisions made and acted on.

Standing Versus Temporary Authorities

The unit is conducting a bilateral security cooperation training event with a partner nation that had previously contributed forces in Afghanistan. As the exercise gets underway, the liaison officer from the partner nation asks why they had access to systems and information in Bagram that they don't have for this exercise. In a key leader engagement, the commander of the partner nation asks the senior Army commander if something has changed about the nature of the relationship between the two nations.

The senior Army commander explains to her foreign counterpart that just as with authorizations for increased spending and increased Army end strength, increased or enhanced disclosure authorities for named and contingency operations end with the conclusion of those activities. The senior Army commander informs her counterpart that this is not an Army decision, but a national decision grounded in national policy for disclosure authorities and exigent circumstances.

3-20. In the **Standing Versus Temporary Authorities** vignette, the senior commander answers the differences in disclosure. The entire organization must clearly understand the disclosure authorities according to country, category of information, and classification level. These authorities dictate the production of information through the WFR process. The U.S. Government communicates with partners which sharing agreements they are using depending on the circumstance. It is the policy of the U.S. Government to temporally expand authorities (such as fiscal and disclosure) when conditions warrant.

Informed Consent

A staff officer is stationed at an Army Service component command. The Army has been designated as the lead for a joint/combined task force mission to provide the initial humanitarian relief for earthquake victims in Bandaria. The Army has a bilateral intelligence sharing agreement with the Bandarian Army. The neighboring countries of Kwladar and Zantos will also be providing forces to augment TASK FORCE GROB's initial efforts on the ground.

Force protection concerns relate to the initial introduction of Army units into the area of responsibility, and Bandaria agreed to provide intelligence threat information related to indications and warnings to U.S. Army forces. The staff officer realizes the indications and warnings information is of likely interest and benefit to the forces from Kwladar and Zantos as well and wants to ensure those nations have a common situational awareness of potential threats. The staff officer coordinates with the Bandarian Army to share the indications and warnings with forces from Kwladar and Zantos.

3-21. In the **Informed Consent** vignette, the staff officer decides whether to share information. Formal information sharing agreements exist to serve the specific purposes of the named participants. Staffs and planners never assume that any partner nation grants permission to disclose its information to third parties. The same rules and requirements to obtain the permission of the proponent prior to disclosure extend to foreign partner information as well. The process must be acknowledged and understood across the entire organization, especially in circumstances in which the composition of the multinational effort is subject to expanding. Planners must understand the authorities and agreements before executing any operation. It is counter-productive to ask for additional foreign partner participation if issues in sharing foreign government information exists, thus degrading partner contributions to the combined effort.

The Absence of NOFORN Does Not Automatically Equal "YESFORN"

You are preparing briefing slides related to unit readiness. The security classification guide states that when this information is in the aggregate, it is marked SECRET. You know that staffs will forward this information to a higher headquarters and the foreign military personnel exchange program participants who work there.

You are unsure if those military personnel exchange program participants should have access to this classified information. You choose to potentially err on the side of caution and mark the slides NOFORN.

3-22. The last vignette demonstrates a potential misuse of the NOFORN caveat. In many instances, military personnel exchange program participants require access to readiness information to perform the mission the Army expects of them. However, the absence of a NOFORN marking does not automatically mean the information can or will be shared with a foreign partner. Prior to any disclosure, a foreign disclosure officer or representative needs to make a disclosure decision or determination.

3-23. Constraints and limitations are addressed initially during mission analysis. The same external factors influence potential courses of action as they retain the same influence on the products and information required to develop and implement a course of action. Knowing these constraints and limitations, where they come from, and why they exist greatly reduces organizational errors and false starts in information sharing through the WFR process.

This page intentionally left blank.

Chapter 4

Overview of the Write for Release Process

This chapter provides an overview of the entire WFR process. First, the chapter discusses the overall WFR process as an organizational process. The rest of the chapter describes each step within the WFR process. This WFR process is continuous and cyclical. Units can start, stop, and restart at any step of the process.

AN ORGANIZATIONAL PROCESS

4-1. Partner nations operating in an MPE expect to share information with other partners. The WFR process is not a linear process but cyclical with no defined start or end points due to the anticipated high volume of information sharing requests. Additionally, the WFR process is not solely executed by a security manager, foreign disclosure officer or representative, or someone within the intelligence community. Every partner nation, staff section, or working group needs plans to execute the WFR process as it applies to the information they have available. There is a reasonable expectation that partner nations will also share information. Effective actions during planning, preparing, executing, and assessing operations require continuous information sharing between partners. The WFR process enables organizations operating within an MPE to share information more effectively and efficiently. Staffs can apply this process to partners with which the U.S. Army is currently working or planning to work with in future operations.

4-2. Figure 4-1 on page 4-2 depicts the five-step WFR process. The five steps are requirements determination, requirements analysis, pre-production, production, and disclosure and dissemination. Typically, the WFR process is continuous due to the anticipated high volume of information sharing requests when operating within an MPE. However, instances occur where the process can be linear, such as when answering a one-time request for information. For the purposes of this publication, the WFR process is applied to operating within an MPE.

4-3. The information sharing requirements that result from operating in an MPE drive the WFR process. When operating within an MPE, staffs must synchronize information sharing and the WFR process to ensure information sharing requirements are met.

REQUIREMENTS DETERMINATION

4-4. Sharing information with partners is an operational imperative. This necessity is one the Army addresses and meets through the WFR process. Although "write" denotes the production of a physical document, the WFR process includes the same actions for oral or visual disclosures.

4-5. Requirements drive information sharing with partners. National, DOD, and U.S. Army foreign disclosure policies mandate that the shared information produces a benefit to the U.S. Government. Therefore, a concept of benefit or risk versus return calculus will always be the foundational requirement. (See chapter 5 for more on risk versus return calculus.) National, DOD, and U.S. Army policies allow individuals designated as disclosure authorities to assess the benefit of sharing pieces of information and deciding the appropriate information to disclose.

4-6. Staffs begin each plan to share information with reviewing governing authorities by country, the category of information, and a classification level. Losing sight of these constraints creates risk. If constraints are not followed, later in the planning process higher staffs may discover that information planned to be shared is not supported by the disclosure authorities.

Write for release is a continuous process that is made up of multiple sub-processes. In turn each sub-process will drive other sub-processes, have distinct outputs, or both.

Figure 4-1. The write for release organizational process

4-7. Staffs consider organizational requirements to share information. These requirements may be either specified or implied. Requirements to share organizational information includes information that originates from within and outside of an organization. Frequency and format requirements from internal or external organizational requirements direct production requirements.

REQUIREMENTS ANALYSIS

4-8. The requirements analysis process follows a well-defined logic trail. It is best articulated and understood as a series of statements or as questions that are asked and answered. The answers inform planners of the course of action development, course of action selection, and finally actual pre-production requirements. The requirements analysis process is essential to mission success and requires input from the entire staff. The staff will likely answer questions such as—

- What is the nature or basis for the requirement?
- What are the external factors (constraints and limitations)?
- What does the requirement look like (country, category of information, and classification level)?
- Are these requirements supportable by the current disclosure authorities?
- Based on the analysis above, are the proposed courses of action for information sharing feasible and sustainable?
- If a course of action is feasible, what does it dictate with respect to pre-production and production requirements?

PRE-PRODUCTION

4-9. As shown in Figure 4-1 on page 4-2, the WFR process is a series of interrelated sub-processes constantly in action. The interrelationship among activities is best demonstrated by many of the pre-production activities. These constant pre-production activities include—

- Education across the organization on information sharing for the purpose and commander's intent.
- Education across the organization on the basic tenants of foreign disclosure.
- Education across the organization on information security fundamentals (markings).
- Provisions made across the organization for regular coordination or working groups.

4-10. Product specific pre-production activities include—

- Knowledge of the applicable disclosure authorities by country, category of information, and classification level.
- Knowledge of number and versions of the product to be produced such as one version for the United Kingdom and one version for France.
- Advanced coordination for permission to disclose information originated or classified external to the organization.
- Advanced affirmative disclosure determination.

PRODUCTION

4-11. Prior to this publication, the WFR process historically started with production. This production frequently resulted in an "edit for release" approach based on products and information that already existed for U.S.-only audiences. By executing the WFR process, staffs simplify production efforts and decrease timelines. As a continuous organizational process, production becomes focused and timely. Then authors and analysts can deliberately construct products with the following, agreed upon criteria:

- Knowledge of the purpose and commander's intent of the intended audience.
- Knowledge of the drivers that influence production deadlines.
- Knowledge of the required markings.
- Knowledge of advanced affirmative disclosure determination decisions.
- Knowledge of disclosure as well as disclosure and dissemination plans.

DISCLOSURE AND DISSEMINATION

4-12. Disclosure and dissemination are two related terms. In national, DOD, and Army policies, disclosures can come in three forms or mediums:

- Oral. Recipient is only told the information.
- Visual. Recipient is shown the information for temporal study.
- Documentary. Recipient receives the information conveyed in physical form for permanent retention.

Note. The intelligence community uses the term *release* to denote a documentary disclosure.

4-13. While the form or medium of disclosure reflects a disclosure decision (what can other partners know), it also addresses how partners get information. Because of the increased reliance on electronic transmissions, plan dissemination as part of production. Staffs plan for dissemination by acknowledging and accounting for the challenges partners may face with compatibility to U.S. systems or networks.

ASSESSMENT

4-14. The WFR process requires assessments of each step to determine if the information being shared within an MPE meets the partners' information requirements. The WFR process is a series of interrelated and continuous processes. As such, it is essential that the commander and staff view their assessment efforts in the same manner. Commanders and staffs should consider measures of performance (MOPs) and measures of effectiveness (MOEs) during the assessment step of the WFR process.

Chapter 5
Requirements Determination

This chapter discusses the first step in the WFR process: requirements determination. The WFR is a continuous, cyclical process. While operating within or preparing to operate in an MPE, the staff determines the information sharing requirements. This chapter first demonstrates how to apply the risk versus return calculus when determining information sharing requirements. The chapter then provides examples of drivers for the information sharing requirements determination. Lastly, the chapter discusses understanding the requirements and their impacts on the staff.

RISK VERSUS RETURN

5-1. In July 1971, the National Security Decision Memorandum 119, in part, established—

- Classified military information is a national asset that requires protection.
- Classified military information may be shared with foreign governments and international organizations when there is a “clearly defined advantage to the United States.”
- Sharing information provides an expected advantage to the U.S. that outweighs the risk of compromise of U.S. military secrets.

5-2. The policy provision for a “clearly defined advantage,” was intentionally not expanded because it expected people to exercise the policy judiciously. The provision allows for great latitude for individuals formally delegated as an authority to assess the risk versus the return. Practical justifications of this clearly defined advantage include, but are not limited to—

- Garnering and maintaining international support for and during active military operations.
- Improving interoperability and compatibility with partners.
- Enhancing Army capabilities through cooperative research and development.
- Building and maintaining relationships that reassure allies and partners while dissuading potential adversaries.

When applying the risk versus return calculus, the staff should consider and ensure that the benefits (return) of sharing information, outweigh the risk. This is the basis for the WFR process.

DRIVERS

5-3. A driver is an authoritative source, directive, or guidance. These drivers determine whether staffs can and should share information. Additionally, drivers provide justification when applied to the risk versus return calculus as they provide a clearly defined advantage to the Army forces operating in an MPE. These drivers include, but are not limited to—

- The *National Security Strategy*.
- The *National Military Strategy*.
- Campaign Plans.
- Operation plans.
- Commander’s intent and guidance for information sharing.

6-4. These drivers identify organizations affected by, or interested in, the desired outcomes from U.S. interactions with partners when operating in an MPE. The objectives and desired outcomes become actionable efforts linked to DOD and U.S. Army security cooperation programs. (Refer to DA Pam 11-31 for a complete list of these programs.) These programs are examples of information sharing requirements drivers for the WFR process when applied to an MPE. Some examples include—

- The North Atlantic Treaty Organization.
- The American, British, Canadian, Australian, and New Zealand (ABCANZ) Armies Program.
- The foreign liaison officer program.
- The international visits program.
- The military personnel exchange Program.
- Training and doctrine staff talks.
- Army-to-Army staff talks.
- The Military Committee Land Standardization Program.
- The Army Global Civil-Military Emergency Preparedness Program.
- The International Cooperative Research, Development, and Acquisition Program.

5-5. Figure 5-1 is an example of how the staff derives the WFR process requirements from the drivers. In this example, Bandaria is the intended audience, and the effort is a combat training center rotation. Additional factors for consideration are time and duration.

5-6. As mentioned in Chapter 2, identifying the WFR process requirements is a staff responsibility. The various staff sections leverage their subject matter experts to—

- Forecast information requirements from partner nations.
- Obtain information sharing restrictions that the partner nation has for information they originate.
- Obtain information requirements that the partner nation has for information originated outside their organization and for coordination requirements.

5-7. Since the requirements determination process is continuous, the staff remains prepared for other sources of requirements. These are best described as directed, inherent, or directed by planning. Understanding the sources of the information sharing requirements allows the staff to quickly respond and satisfy these requests or requirements. Paragraphs 5-8 through 5-10 provide examples of directed, inherent, or directed by planning requirements.

5-8. Examples of directed requirements include the following:

- Specified tasks to prepare leaders for key leader engagements with their counterparts. The staff will need to know proposed agenda items, anticipated topics to be brought up by the leader's counterpart, and agreed-to actions from previous meetings.
- Specified tasks to identify information proposed for disclosure as part of the request for visit authorization (known as RVA) process in support of the international visits program. In the request for visit authorization, the information authorized for disclosure is determined by the purpose of the visit and drives the WFR process.
- Tasks for an organization to respond to a formal request for information originating from a partner nation.

5-9. Examples of inherent requirements include the following—

- Information required by the military personnel exchange program. With military personnel exchange program participants, the position description determines the information sharing requirements. The position description (what the military personnel exchange program is expected to do for the U.S. Army) is mutually agreed upon between the U.S. Government and the military personnel exchange program country.
- Information required by the foreign liaison officer program. With foreign liaison officer participants, the position description determines the information sharing requirements. The position description (what the foreign liaison officer is expected to do for his or her government) is mutually agreed upon between the U.S. Government and the foreign liaison officer's country.
- Information required as part of active participation in an MPE. The mission partners have agreed upon terms of reference, goals, and common doctrine or procedures.

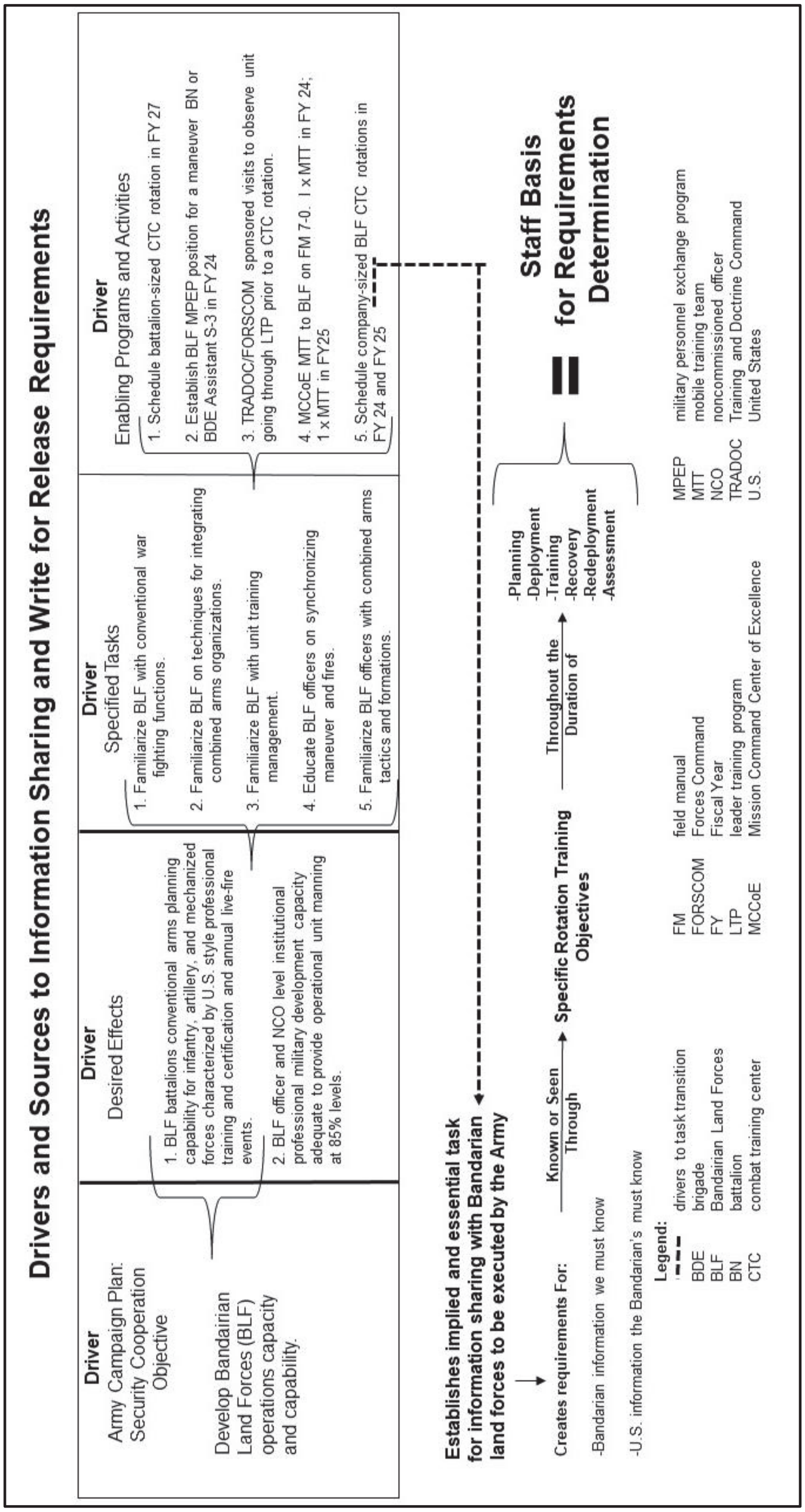

Figure 5-1. Illustration of mapping

5-10. Planning staffs identify the "directed by" planning information sharing requirements during a deliberate planning process. As staffs plan, they implement the WFR process and identify information sharing requirements as early as possible. The scenario depicted in Figure 5-1 illustrates "directed by" planning requirements. Other efforts that fit this category include—

- Approved contingency or operation plans.
- Exercise directives for warfighter type events.

CAPTURING AND CATEGORIZING REQUIREMENTS

5-11. As the commander and staff begin to identify information sharing requirements, they understand both the source of the requirement and the disclosure agreements. Understanding the requirement drivers (listed in paragraphs 5-3 and 5-4) sets the foundation for the WFR process.

5-12. The commander and staff also begin to capture potential impacts for further analysis. These include but are not limited to—

- The anticipated frequency of the sharing or the schedule that will drive the process.
- The anticipated type of product.
- The anticipated medium of disclosure (oral, visual, or documentary).
- The anticipated plan for dissemination of the information.
- The possibility of needing to prepare multiple versions of products.
- The potential information sharing requirements by countries not yet specified.

5-13. The potential information sharing requirements by countries not yet specified is significant enough that it warrants mentioning, especially as applied to requirements from the "directed by" planning category. Units frequently conduct events in this category as part of a long-range plan. When applied to warfighter or training events, subsequent efforts build on previous iterations, often expanding the membership base of partners. Lessons learned or after-action reviews that have been approved for disclosure are likely to be of value and interest to subsequent partners and result in an information sharing requirement.

Chapter 6

Requirements Analysis

This chapter provides information about identifying and analyzing information necessary to inform and shape the WFR process. Success with these early efforts will pay dividends as the staff develops and implements the information sharing plan. The requirements analysis process builds on the staff's previous efforts to identify requirements. The chapter first provides a method for the staff to map the information sharing requirements back to the source. The WFR process requires proper analysis of the information sharing requirements. Then the chapter provides examples of criteria against which the information sharing requirements should be analyzed. This last discussion describes the continuous analysis of information sharing requirements performed by the staff.

REQUIREMENT MAPPING

6-1. Since the WFR process is an organizational process, each staff maps its potential requirements back to a source. This ensures that the organization adheres to the fundamental national disclosure policy requirement to assess the risk for the return. Mapping helps the staff maintain visibility on specific goals and objectives throughout the WFR process. Mapping can be done in several ways. One way includes building a spreadsheet to identify pertinent details that might become potential disclosure requirements. See Figure 6-1 on page 6-2 for one example of a WFR planning tool in a spreadsheet style.

6-2. Using Figure 6-1 on page 6-2, the staff identifies partner nations who are subjects of this analysis after identifying the source. Just thinking long range and identifying a partner as a potential audience does not obligate the U.S. Government to share information with them. Early identification of potential audience members proactively informs subsequent decisions and efforts. Column B in Figure 6-1 lists the United Kingdom, France, and Germany as these countries.

An initial staff support tool at this point, could be nothing more than a spreadsheet that helps to identify and record potential disclosure requirements for analysis

	A	B	C	D	E	F
	Driver/Source Goal/Objective	Country(ies)	Specific Information Requirements	Category(ies) Of Information	Proponent/Owner/ OCA of the Information	Anticipated Classification Level
1	Army Campaign Plan	UK	Force Structure Munitions Order of Battle	1,5,6	V Corps	S//REL UK
2	Army Campaign Plan	UK	Force Structure Munitions Order of Battle	1,5,6	V Corps	S//REL UK
3	Army Campaign Plan	Germany	Force Structure Order of Battle	1,5,6	V Corps	S//REL DEU
4	Army Campaign Plan	France	Force Structure Order of Battle	1,5,6	V Corps	S//REL FRA
5	Army Campaign Plan	France	Force Structure Order of Battle	1,5,6	V Corps	S//REL FRA
6	Army Campaign Plan	UK, France	Force Structure Order of Battle	1,5,6	V Corps	S//REL UK, FRA
7	Army Campaign Plan	UK, France, Germany	Force Structure Munitions Order of Battle	1,2,5,6	V Corps	S//REL NATO

Figure 6-1. A sample write for release planning tool

6-3. The staff then identifies specific WFR requirements. The greater the specificity, the greater the chance an accurate assessment will be made. (Figure 6-2 illustrates differences in such details for the WFR process.)

GOOD	BETTER	BEST
Doctrinal information	Doctrinal information to facilitate precision long range fires	ATP 3-09.34 ATP 3-09.60 ATP 3-09.70

Figure 6-2. Descriptions by detail for write for release

6-4. Foreign disclosure representatives advance the WFR process by ensuring that their staff sections know and understand the disclosure policy. The basis of the disclosure policy includes delegated authorities, partner nation categories of information, and classification levels. A way to ensure this from the start is for the staff to capture their requirements in this manner from the outset. See Categories of Information in column D in Figure 6-1 on page 6-2.

6-5. For information originating or classified external to the organization, staff members need to know the source of this information. They require the source to coordinate permission to share. Column E in Figure 6-1 on page 6-2 shows V Corps as the owner of the information.

6-6. Finally, the staff makes an initial assessment regarding the classification of the information by consulting the relevant SCGs. The foreign disclosure representatives coordinate with the command security manager for this information. See Column F in Figure 6-1 on page 6-2 for the anticipated classification level of the information to be released.

6-7. The staff addresses all information in Figure 6-1 when implementing the WFR process. Friction and risk to the mission increase the longer the staff waits to use these details. When determining risk for return, all staff members need to know—

- Disclosure policies.
- The information originator.
- Classification of information.

CRITERIA FOR CONSIDERATION

6-8. Next, the staff assesses and analyzes the initial requirements against a set of criteria. At a minimum, this criterion includes the following:

- Disclosure authorities by country, category, and classification level.
- Commander's intent for the WFR process.
- Planned missions for foreign partners.
- Permissions and authorities granted for information originating outside of the organization.
- Impacts of external forces.
- Information requirements articulated by partners.
- Anticipated frequency as it relates projected schedules of meetings and decision cycles.
- Planned means of disclosure and dissemination.

6-9. Figure 6-3 on page 6-4 illustrates a method to create and complete an analysis matrix for information sharing. Typically, the top row provides those items the staff considers for planning. In this example, the considerations include those that support the information sharing, those who enable the information sharing, and those who will execute the disclose or dissemination plan. The first column often addresses the requirements. In this example the requirements include the planned role and mission for the partners, specific information requirements, and ability to produce the product. A staff officer jots such a matrix to keep track of requirements to share information with others. The remaining columns are yes or no questions that provide the staff officer with reminders of completed or incomplete coordination.

Requirement \ Planning Consideration	Supported by current or anticipated disclosure authorities	Enabled by outside permissions	Executable by planned battle rhythm disclosure and dissemination plan
Planned role or mission for partners	YES	YES	YES
Specific information requirements	YES	YES	YES
Ability to produce a single version of required products for all	NO	YES	NO

SAMPLE

Figure 6-3. Sample write for release analysis matrix

6-10. The requirements analysis process is best articulated and understood as a series of statements or as questions that are asked and answered. The answers to the questions inform the course of action development, course of action selection, and finally actual pre-production requirements. The staff ensures that each information sharing course of action in the WFR process is feasible, acceptable, suitable, and distinguishable. Staffs consider the following when developing WFR courses of action:

- If planning considerations do not permit the proposed nation to participate in the MPE, consider whether that nation can be an observer.
- If the planned role is not supportable, consult with the partner to identify another mutually valued added role or contribution that is supportable.
- If information sharing and disclosure authorities are not supportable for all countries at a common, proposed level, either work from a lower common level or plan to produce various versions of products to share as required.
- If technical issues (such as system compatibility) hinder information sharing and dissemination, plan for and establish mutually agreed upon mechanisms and procedures to link the shareable information for each partner to the method of dissemination. (See Appendix C for troubleshooting issues.)

SUBSEQUENT EVALUATION AND ANALYSIS

6-11. Figure 4-1 (on page 4-2) depicted and categorized the WFR process as a series of continuous and interrelated organizational processes. The commander and staff plan for analyzing and evaluating their requirements in a similar continuous manner. Changes that occur in an MPE require continuous evaluation and analysis. It is important for the commander and staff to know, understand, and account for how change impacts the WFR process. Categories of changes include the following:

- Changes in composition of the force.
- Changes in mission.
- Changes in disclosure authorities.
- Changes in capabilities.

6-12. Changes in composition of the force refers to a new partner nation joining or leaving an MPE. When this occurs, the staff reworks its evaluation and analysis efforts. Other planning considerations include—

- Potential remarking of information previously disclosed as part of the existing effort.
- Coordination with existing partners to share their information with the new partner.

6-13. Changes in mission refers to new, added, deleted, or modified tasks added to the overall mission. Changes to tasks create changes to information requirements.

6-14. Changes in disclosure authorities occur with an interagency exception to national disclosure policy and an issued record of action. Staffs exercise caution when applying the disclosure authorities contained in an approved record of action since the disclosure authorities tend to be very specific in nature and frequently contain additional provisions that must be adhered to.

6-15. Changes in capabilities occur when adding a new information category to the effort. These changes may expose partners to unplanned technologies and capabilities. Changes in capabilities also occur when making changes to networks or systems moving information between partners. (See Appendix A for more information on categories of information.)

This page intentionally left blank.

Chapter 7

Pre-Production

This chapter provides the basic tenants of the pre-production step of the WFR process. Pre-production involves gathering the tools to ensure that released products comply with disclosure authorities. This chapter first discusses the application of an advanced affirmative disclosure determination as it applies to the WFR process. The chapter then provides the goals for pre-production.

ADVANCED AFFIRMATIVE DISCLOSURE DETERMINATION

7-1. The *National Disclosure Policy*-1 requires that the formal delegated authority make a disclosure determination or decision prior to sharing information with partners. The policy allows for some leeway for methods and timing of the decision. Delegated disclosure authorities have the following options:

- Make decisions during the WFR process as it relates to each individual product or event and as it relates to a particular partner.
- Make an advanced affirmative disclosure determination (A2D2).

7-2. A2D2s reflect that a designated disclosure authority analyzed requirements, conducted risk versus return analysis, and determined, in advance, the information for which they are the disclosure authority. During the WFR process, delegated disclosure authorities reduce the time decisions to release and the actual release of information by using an A2D2. Examples of these decisions include the following:

- Authority for disclosure of a particular category of information and classification level.
- Authority for a particular and well-defined set of circumstances.
- Authority for a particular time frame.
- Authority to make an A2D2 to share the previously identified information without requiring any further foreign disclosure review.

7-3. The A2D2 is best applied—

- From senior levels (Army Command, Army Service component command, or direct reporting unit) to influence the subsequent major subordinate command efforts.
- For formal and well-defined security cooperation events and programs such as exercises, the military personnel exchange program, and the foreign liaison officer program.
- When expecting a high volume of frequent or regular disclosures.
- To well-defined and unlikely to change requirements (by country, category, and classification level).

7-4. The A2D2 does not—

- Eliminate the requirement to coordinate for permission to disclose information originated, classified, or both by another organization.
- Eliminate the need to comply with the provisions contained in SCGs, mandates by a caveat in a partner agreement, or information security marking guidance.

7-5. National level disclosure guidance provides the authority to determine disclosure in the absence of an A2D2. This guidance includes disclosure applied by country, category of information, and classification level.

7-6. Prior to the production of specific products, regardless of the timing of the disclosure determination, the staff needs to know answers to the following questions:

- What partner nation groupings for disclosure exist?
- How many versions of the product are required?
- What is the projected timeline and frequency of production and dissemination of the product?
- What is the timing of permission obtained for information originated, classified, or both external the organization? Knowing this in advance allows for conditional production as opposed to waiting to start until after obtaining permission.

GOALS OF PRE-PRODUCTION

7-7. The goals of pre-production efforts are—

- Compression of timelines for production.
- Timely and correct production of products.
- Meeting the WFR requirements.

As the staff works through the assessment process, they pay particular attention to changes or recommendations which may cause another round of pre-production activities.

Chapter 8
Production

This chapter provides information for the staff to use during the production process. A2D2 discussed in Chapter 7 reduces the efforts required by the staff during the production step of the WFR process. At the production step in the process, the staff focuses its efforts on timely and accurate marking, change management, and mapping the intended means of disclosure and distribution.

MARKING

8-1. The accurate marking of documents and products per a disclosure determination is a specified and essential task. As noted in paragraph 3-13, a releasable to (known as REL TO) marking indicates previous disclosure or imminent disclosure to a partner. A releasable to marking becomes problematic when the product contains both previously disclosed information as well as new information proposed for disclosure.

8-2. Historically, a foreign disclosure officer made the final marking of documents in the production process. The volume of information and the limited personnel making foreign disclosure decisions created delays in sharing information. Disclosure is and was an organization-wide responsibility that had been placed on the foreign disclosure officer. To correct this, a successful organization currently uses the WFR process as part of the information sharing program.

8-3. The four marking scenarios provide examples of how to mark, gain approval, and disseminate information based on sharing requirements. In courses of action 1 and 2, the approval authority reviews, marks, and approves the information. In courses of action 3 and 4, the proponent or information owner recommends the appropriate classification marking based on national disclosure authorities, SCGs, and information sharing requirements. WFR is designed to share information in an efficient and timely manner, as demonstrated in courses of action 3 and 4.

Four Marking Scenarios

Course of action (COA) 1: Information not yet approved for disclosure, only annotated in some manner that indicates disclosure is desired. This annotation is not marked as "REL" to avoid confusion with previously approved information. Once the disclosure authority makes a disclosure determination and notifies the proponent of the decision, the proponent portion marks the document "REL" for disclosure.

COA 2: Information not yet approved for disclosure, only annotated in some manner that indicates disclosure is desired. This annotation is not marked as "REL" to avoid confusion with previously approved information. Once the disclosure authority makes the disclosure determination and notifies the proponent of the decision, the foreign disclosure officer marks the document "REL" for disclosure.

COA 3: Information not yet approved for disclosure is marked with the intended "REL" marking, only this proposed marking is in RED and BOLD for ease in identification. Once the disclosure authority makes the disclosure determination, the proponent is notified, and the proponent marks the document for disclosure by changing the RED and BOLD DRAFT markings to BLACK and NORMAL.

COA 4: Information not yet approved for disclosure is marked with the intended "REL" marking, only this proposed marking is in RED and BOLD for ease in identification. Once disclosure determination is made, the disclosure authority notifies the proponent, and the foreign disclosure officer marks the document for disclosure by changing the RED and BOLD DRAFT markings to BLACK and NORMAL.

8-4. In the vignette examples, course of action 4 presents potential gains in time as well as ensured positive control over the process. As mentioned in paragraph 8-2, how this is accomplished remains an organizational-level decision. Regardless, those involved need to use consistent marking methods and needs to complete them promptly to avoid unnecessary delays.

CHANGE MANAGEMENT

8-5. When information changes, production efforts resulting from recurring requirements and updated on a regular basis often experience delays due to an organizational decision. Such delays then require additional disclosure reviews.

8-6. Authorities under which the U.S. Army operates are delegated by nation, category of information, and classification level. Staffs consider the authorities when deciding if an additional review is necessary. A mandatory additional review happens when a significant change occurs to the nation, category of information, or classification level. There is no need for an additional review without significant changes. Examples of significant changes include—

- Adding a new or additional partner nation to the releasable designation.
- Adding a new or additional category of information not yet approved for disclosure.
- Increasing the level of classification of the information.

8-7. Managing the changes during production also involves the re-marking of previously disclosed information to a larger or expanding group of partners. When a marking change is needed, staffs disseminate the revised marking guidance to all staffs through the foreign disclosure representatives. Staffs make every effort to eliminate potential foreign disclosure review delays with work that others can do using the WFR process.

MAPPING TO DISCLOSURE AND DISTRIBUTION

8-8. Information is useless if it does not get to those who need it when they need it. Before the staff produces information, it needs to know the disclosure and distribution method (oral, visual, or documentary).

8-9. Very seldom do Soldiers limit themselves to only oral or verbal disclosures. When sharing information only verbally, the staff continues to work through the production step of the WFR process. Planning for the production step includes planning time for additional information to guide and inform the commander and staff members making the disclosure. Examples are, but are not limited to, the following:

- Awareness and understanding of the *National Disclosure Policy*-1's false impressions.
- Anticipating follow-on questions and potential disclosure issues associated with answers.
- Preparing to record requests for information.

8-10. Visual disclosures rarely occur without a verbal conveyance of the shared information. In most cases, disclosures are approved for "oral and visual." Visual disclosure means the information is available for "temporal study" without an established time or duration specified. The only restriction is that the information disclosed is not transmitted for permanent, physical retention. When oral and visual disclosures are made, production requirements include—

- Guidance from the staff to the audience regarding permissions and prohibitions for taking notes and photographs.
- Proper storage of the information during temporal study and analysis.

8-11. Documentary disclosure means information is physically transferred for permanent, physical retention. While the words documentary disclosure denotes documents, documentary disclosure also includes the physical transfer of arms, munitions, and equipment through any number of security assistance efforts. Planning for documentary disclosures includes the following production requirements:

- Guidance from the staff to the audience on transfer and storage requirements.
- Internal guidance to and from the staff to facilitate machine ingestion or transfer to the partner nation.

This page intentionally left blank.

Chapter 9
Disclosure and Dissemination

This chapter provides information to help staffs identify actions and activities for the disclosure and dissemination step of the WFR process. Chapter 8 includes some of these actions and activities as well. Soldiers use the mnemonic SHARE (stick, have, always, record, and emphasize) as a guide.

STICK

9-1. The first step in the mnemonic SHARE is stick. Staffs stick to the plan for the product and the audience. Follow the plan means to stick to the plan. Pre-production and production planning include mapping or connecting the product to the means of distribution. During this mapping of the product to the distribution means, Soldiers establish and communicate expectations for format and develop timelines for production and distribution. Soldiers follow these timelines and meet these expectations during disclosure and dissemination.

HAVE

9-2. The second step in the mnemonic SHARE is have. Soldiers have the resources in place. Transfer of information or products requires resources. Resources often require prior coordination. Without the coordination in place, delays occur in final products reaching final recipients. Soldiers get resources in place by—

- Assigning a robust number of foreign disclosure representatives to match partner consumption plans and requirements.
- Properly identifying and allocating systems to match partner consumption plans and requirements.
- Matching partner consumption plans and requirements to physical security and storage requirements.

ALWAYS

9-3. Always is the third step in the mnemonic SHARE. Soldiers always have an analog backup plan in place. Information is the lifeblood of making decisions. When systems or networks for the transfer of information falter or experience problems, sharing information and making decisions continue. Soldiers have primary, alternate, contingency, and emergency methods of sharing information. The primary method is likely a direct, digital transfer using a common system. An alternate method might involve using an interface between systems that authenticates the authority to receive and transmit information. A contingency method could be printing information on paper with a courier delivery to partners or by passing it through assigned foreign liaison officers. An emergency method may be using radios and an encryption cypher code to share information. Staffs always provide a human or a procedural solution to a technological problem.

9-4. The MPE has three interoperable, problem-solving dimensions to help staffs plan for the eventuality of a technological failure, whether it be a failure of power, cybersecurity, or mechanics. Any of these failures will trigger the commander or staff to activate their primary, alternate, contingency, and emergency (known as PACE) plan for WFR. Table 9-1 on page 9-2 identifies solutions divided into the dimensions of human, procedural, and technical.

Table 9-1. The primary, alternate, contingency, and emergency methods for write for release

Type	*Method and mode to share*
Human solutions	Primary – trainers for common system usage
	Alternate – trainers for interface usage
	Contingency – courier
	Emergency – trainers for cypher usage
Procedural solutions	Primary – joining, membership, and exiting instructions for common digital system
	Alternate – joining, membership, and exiting instructions for interface
	Contingency – procedure of who couriers and when
	Emergency – cypher encryption tools
Technical solutions	Primary – common digital system
	Alternate – interfacing software
	Contingency – copier machines
	Emergency – voice communications

9-5. Staffs always make analog plans for the following:

- Temporal hard copy printing, distribution, and storage. Staffs plan to resource General Services Administration (known as GSA) approved safes. Staffs then maintain document records in accordance with information security regulations.
- Make provisions for approved and secure removable media aiding the manual transfer of information on a temporary basis.

RECORD

9-6. The fourth step in the mnemonic SHARE is record. Staffs record the results. The *National Disclosure Policy*-1 mandates recording the results of transfers. Equally important, recordkeeping is a critical component of both decision and assessment processes. Recordkeeping includes the following:

- Keeping track of information shared with partners negates the need to repeat the disclosure review and approval process for the same information in the future. Once the information has been designated as releasable to and shared with a particular country, that decision applies to further instances. While a releasable to precedence does not obligate the U.S. Government to continue to share, it is a legitimate basis to continue sharing the same subject information.
- The assessment process requires staffs to track shared information with an emphasis on the medium (oral, visual, or documentary), the timelines, volume, and value or utility. It is far easier to document information sharing while it is occurring rather than after the fact.

EMPHASIZE

9-7. Lastly, the mnemonic SHARE ends with the step emphasize. Staffs emphasize feedback and process improvement from all parties concerned. Feedback from partners informs future sharing of information either by process or means. Emphasizing feedback is a process for improving interoperability with our partners in an MPE.

Chapter 10

Assessment

This chapter discusses the MOPs and MOEs that should be considered during the assessment step of the WFR process. Assessments of each step of the WFR process are critical in determining if the information being shared within an MPE is meeting the partners information requirements.

MEASURES OF PERFORMANCE

10-1. A *measure of performance* is an indicator used to measure a friendly action that is tied to measuring task accomplishment (JP 5-0). For the purposes of the WFR process, MOPs answer the question "Is the right information shared with the right partner in a timely manner?" Currently, there are no approved Army tasks associated with the WFR process, so each staff needs to establish its own MOPs related to—

- Time to complete the steps of the WFR process.
- Standards for accuracy in marking of information for disclosure.
- Time from receipt of information sharing request to information being disseminated.

While MOPs largely represent an internal process diagnostics set against a quantifiable standard, staffs make provisions to obtain partner feedback in these areas since they represent the customer or ultimate consumer.

MEASURES OF EFFECTIVENESS

10-2. A *measure of effectiveness* is an indicator used to measure a current system state, with change indicated by comparing multiple observations over time (JP 5-0). For the purposes of the WFR process, MOEs answer the question "Are information sharing requirements being met?" In the case of the WFR process, MOEs should be related to the following questions:

- Are the information sharing requirements addressed accurately?
- Is the specific information shared sufficient to meet the requirements?
- Does the current WFR process support the MPE information sharing requirement?

MEASURES OF PERFORMANCE AND EFFECTIVENESS ACROSS THE PROCESS

10-3. The WFR process is a series of interrelated and continuous processes. As such, it is essential that the commander and staff view their assessment efforts in the same manner. This publication provides recommended assessment areas in the form of leading questions and identifies them as either potential MOPs or MOEs. Table 10-1 on page 10-2 is provided as a starting point for the establishment of MOPs and MOEs. It is not an all-inclusive list. Staffs need to modify it to meet their organizational needs. For each question, staffs answer yes or no. Based on the answer, the staff then determines what additional actions to take.

Table 10-1. Write for release measures of performance and effectiveness

The Requirements Determination Process
• Are the right individuals, to include the foreign disclosure officer and foreign disclosure representatives, attending planning conferences and related events? (Measures of effectiveness)
• Are the requirements mapped back to a source or driver that can be articulated or justified? (Measures of effectiveness)
• Did staff mission analysis accurately capture the requirements by nation, category of information, and classification level? (Measures of effectiveness)
• Are forecasted and resourced personnel decisions (number and location of foreign disclosure officer and foreign disclosure representatives) sufficient when assessed by projected and actual throughput of information? (Measures of performance)
The Requirements Analysis Process
• Were the assigned roles and missions of partners consistent with the information they received? (Measures of effectiveness)
• Were requests in enough detail to make rapid and timely coordination for the disclosure of information originating or classified external to the organization? (Measures of performance)
The Pre-Production Process
• Were disclosure determinations, to include advanced affirmative disclosure determinations, made in a timely manner? (Measurement of performance)
• Are the topics covered in the staff education plan sufficient by topic and depth to achieve the desired results envisioned by the commander? (Measures of effectiveness)
• Are the established working groups or similar efforts providing updates and maintaining common situational understanding as envisioned by the commander? (Measures of effectiveness)
The Production Process
• Are documents marked properly when they are first proposed for review and or approval? (Measures of performance)
• Are changes to the organizational makeup (adding partner nations) or organizational requirements (adding categories of information or increased classification level) accommodated consistently with the current schedule? (Measures of effectiveness)
• Is the guidance to the staff and partners on storage and transmission sufficient to make safe and effective transfers while avoiding spillage and other related security incidents? (Measures of performance)
The Disclosure and Dissemination Process
• Does the mission partner network allow information sharing between partners? (Measures of performance)
• When necessary, are procedures and systems sufficient and properly configured for rapid manual transference and input of information? (Measures of performance)
The Assessment Process
• Do provisions exist in shared standard operating procedures that inform the staff of the various time and quality standards they are expected to meet with respect to the write for release process? (Measures of performance)
• For execute orders and similar guidance provided for security cooperation activities, are provisions included for capturing information sharing and the write for release issues as part of the after-action review and lessons learned process? (Measures of effectiveness)
• Are there provisions and guidance that inform the staff of specific data and information to manage and used to inform the assessment process? (Measures of effectiveness)

Appendix A
Categories of Information

Information security marking requirements dictate writers annotate paragraphs to reflect the highest classification level of the information contained in the paragraph. Similar provisions exist requiring writers identify the information category as well. Knowing the categories of information allows commanders and staffs to determine whether the current disclosure authorities support the proposed disclosures. Knowledge of the categories of information offers valuable insight into the proponent (for coordination) and identifying and eliminating the inappropriate use of the NOFORN classification caveat. The U.S. Army adopted the DOD definitions found in Enclosure 2 of DODD 5230.11 to categorize types of information. Use this Appendix as a reference for specific language which tends to be very broad and largely void of the clarifying examples provided in this publication.

CATEGORY 1: ORGANIZATION, TRAINING, AND EMPLOYMENT OF MILITARY FORCES

A-1. Category 1 addresses organization, training, and employment of military forces. A great deal of what an organization does daily involves Category 1 information. Specific examples include—

- Force structure information—(modified) tables of organization and equipment, or Annex A, task order to an operation plan.
- Doctrinal publications.
- Command briefings.
- Training schedules, deployment schedules, and fielding schedules.
- Unit readiness information.
- After-action reviews and lessons learned.

A-2. Soldiers normally do not mark Category 1 information as NOFORN because it does not meet the specific provisions for the accepted use of that classification caveat.

CATEGORY 2: MILITARY MATERIEL AND MUNITIONS

A-3. Category 2 addresses military materiel and munitions. This category includes all military materiel, arms, and munitions procured or controlled, adopted, produced, or used by the DOD. Specific examples include—

- Capability and performance information.
- Information or data regarding the transport, storage, employment, maintenance, or support for military materiel and munitions.

A-4. Category 2 information is covered in detail within system SCGs and typically falls under the purview of the program or product manager for disclosure determinations. Staffs normally do not mark Category 2 information as NOFORN since it does not meet the specific provisions for the accepted use of that classification caveat.

CATEGORY 3: APPLIED RESEARCH AND DEVELOPMENT INFORMATION AND MATERIEL

A-5. Category 3 addresses applied research and development information and materiel. This category involves the element of time within engineering data, general operational requirements, concepts, and military characteristics required to adopt items for production. Until information is approved for adoption, use, or production, it remains Category 3 information. Specific examples can include—

- Concepts under review or development.
- Various aspects and products associated with the Joint Capabilities Integration Development System process.
- Capability and performance information prior to a production decision.
- Draft doctrinal products.

A-6. Category 3 information typically falls under the purview of the program or product developer or manager for disclosure determinations. Staffs normally do not mark Category 3 information as NOFORN since it does not meet the specific provisions for the accepted use of that classification caveat.

CATEGORY 4: PRODUCTION INFORMATION

A-7. Category 4 addresses production information. Category 4 information relates to designs, specifications, manufacturing techniques, and information necessary to manufacture materiel and munitions. This type of information does not include basic assembly information. Disclosure authority for Category 4's classified military information is with the highest levels of the DOD and is not something with which a commander or staff would work.

CATEGORY 5: COMBINED MILITARY OPERATIONS, PLANNING, AND READINESS

A-8. Category 5 addresses combined military operations, planning, and readiness. The key to understanding when something is Category 5 information is the application of the information to a specific purpose. Category 5 is applied when the purpose is to plan, ensuring readiness, and providing support for achieving mutual force development goals, tactical operations, and exercises. Category 5 does not include strategic plans and guidance or North American defense information as North American defense information is its own category.

A-9. Category 5 information is very broad because it includes information previously categorized as Category 1 and Category 2. For practical purposes (mission partner activities), staffs normally do not mark Category 5 information as NOFORN as it does not meet the specific provisions for the accepted use of that classification caveat. Marking Category 5 information as NOFORN is self-defeating because the intent of the category itself is improving interoperability between partners.

CATEGORY 6: ORDER OF BATTLE

A-10. Category 6 is the order of battle. A combination of content and purpose underlies Category 6 information. Category 6 information involves the identification, strength, command structure, and disposition of personnel, units, and equipment located in territory under the jurisdiction of the recipient government (host nation) or otherwise direct concern. Category 6 aims to inform and create awareness on the part of the recipient country (partner nation) as to the nature or purpose of U.S. forces in their country or area of concern. Examples include—

- Information necessary to obtain overflight permission.
- Information necessary to obtain ground transit permission.
- Information necessary to support mutual force protection activities.

A-11. For practical purposes (partner activities), staffs normally do not mark Category 6 information as NOFORN since it does not meet the specific provisions for the accepted use of that classification caveat. Marking Category 6 information NOFORN is self-defeating because the intent of the category is to increase awareness of the partner nation.

CATEGORY 7: NORTH AMERICAN DEFENSE

A-12. Category 7 addresses North American defense. As the name implies, Category 7 information is related to the plans, operations, programs, and projects, to include data and equipment, directly related to North American defense. This category includes information from facets of missile defense to efforts coordinated by the United States Northern Command for consequence management events. The application and use of this category is narrowly defined.

CATEGORY 8: MILITARY INTELLIGENCE

A-13. Category 8 addresses military intelligence. Category 8 information discusses military character as it pertains to foreign nations. This category of information does not include national intelligence or sensitive compartmented information under the purview of the Director of Central Intelligence. Category 8 information is about a foreign nation and not about U.S Army intelligence. Category 8 information does not include—

- Force structure of Army intelligence units (Category 1).
- Category 2 series doctrinal publications (Category 1).
- Capability and performance information for Army intelligence systems and equipment (Category 2).
- Intelligence warfighting concepts and experimentation (Category 3).

When appropriate and consistent with specific and applicable policy guidance, Army staffs designates Category 8 information as NOFORN.

This page intentionally left blank.

Appendix B

Commander's Write for Release Checklist

This appendix provides a modifiable list of questions commanders ask.

B-1. Organizations and their staff benefit from clear and consistent commander guidance. Staff members place greater emphasis on things important to the commander. Table B-1 lists potential items that commanders use to identify their requirements for sharing information with partners. Table B-1 contains potential questions organized sequentially in the order of the WFR process. Commanders answer each question with a yes or no and then act accordingly. The answers to the questions also benefit the staff in addressing the commanders' concerns before receiving guidance. Organizations modify questions based on the mission and partners. Table B-1 provides a starting point when developing the commanders' WFR checklist. Commanders expand or reduce the checklist based on the mission partner, published information sharing requirements, and agreements.

Table B-1. Sample of commanders' checklist

The Requirements Determination Process
• Do the organizational schedules or calendars reflect all the necessary events for the write for release process? • Do running estimates capture the specified and implied tasks for information sharing? • Are the running estimates of a quality to meet commander's guidance for sharing information? • Are pre-briefs scheduled to occur with the foreign disclosure officer before briefing partner unit commanders and the organizational staff members?
The Requirements Analysis Process
• Is the organizational capability and level of authority for 'disclosure' current? • Is the organizational capability and level of authority for 'disclosure' sufficient? • Is the organizational quantity of disclosure personnel, foreign disclosure officers, and representatives current? • Is the organizational quantity of disclosure personnel, foreign disclosure officers, and representatives sufficient? • Was guidance for sharing information provided to the staff? • Were backbriefs regarding the guidance for sharing information conducted to ensure there is a shared understanding?
The Preproduction Process
• Does the staff have and understand the commander's intent for information sharing? • Were advanced affirmative disclosure determinations made when applicable? • Were standards for classification marking communicated? • Are the standards for classification marking followed across the organization? • Is the NOFORN classification caveat being misused? • Who corrected the misuse of the NORFORN classification caveat?

Table B-1. Sample of commanders' checklist (continued)

The Production Process
• Are the organization and its staff addressing classification change management proactively? • Are requests for information addressed at the lowest possible levels? • Is the unit using machine ingestion routinely? • Is the unit using machine ingestion to the greatest extent possible? • Are partners operating on a mission partner network? • Are partners able to share information with other partners using the mission partner network?
The Disclosure and Dissemination Process
• Is information consistently reaching the right audience? • Is information consistently reaching the audience at the right time? • Is information consistently reaching the audience in the right form? • Is recordkeeping sufficient to meet regulatory requirements? • Is recordkeeping sufficient to meet functional requirements?
The Assessment Process
• Do current measures of performance provide the required level of shared understanding? • Do current measures of effectiveness provide the required level of shared understanding? • Are partner nations consulted in a manner consistent with the commander's intent and vision for information sharing?

Appendix C

Troubleshooting Information Sharing Issues

Soldiers will always have legitimate reasons not to share information. At times staffs and organizations cite improper justifications or misinterpret policy and guidance that results in what can be called a "false no." This appendix provides historical examples that Soldiers incorrectly provided to block information sharing. When Soldiers fully and properly understand definitions and policy, their justifications may no longer constitute the "No" justification.

C-1. "The information can't be shared with foreign partners as it's designated as controlled unclassified information (CUI)." Delegated disclosure authority from Headquarters, Department of the Army, Office of the Deputy Chief of Staff G-2 includes provisions to disclose both CUI and categories of military information. By definition and policy, units may share CUI for any lawful governmental purpose, which is any activity, mission, function, or operation that the U.S. Government recognizes as within the scope of its legal authorities. When the justification to share can be mapped back to a valid security cooperation activity, goal, program, or mission that is legally executed by the Army, then the sharing of CUI falls under the umbrella of a lawful governmental purpose.

C-2. "The information is prohibited by a distribution statement." A *distribution statement* is a statement used to mark technical information to indicate the extent of its availability for secondary distribution, release, and disclosure without additional approvals or authorizations. A distribution statement marking is distinct from and in addition to a security classification marking assigned in accordance with Volume 2 of DODM 5200.01 (DODI 5230.24). The foreign disclosure review process constitutes the required "additional approval or authorization" that may be required.

C-3. "The information can't be shared because the equipment, munition, or system is classified." The staff must fully understand what exactly is being proposed for disclosure and what the associated SCG calls for. Soldiers frequently cite that disclosures are prohibited because a country does not have a particular piece of equipment, system, or munition in its inventory. While this is grounded in DOD policy, this policy applies to classified information. Soldiers dealing in and with generalizations about classified systems can frequently respond with an incorrect no.

C-4. "The information can't be shared because it's not covered by the current delegation of disclosure authority letter (DDL), and we lack the authority to share it." If a Soldier offers this justification, recipients need to know if the issue is based on—

- A specific and named prohibition in the DDL.
- The classification of the information against the currently delegated levels.
- The content as a function of the category of information or the absence of a specific positive mention or reference.

While Headquarters, Department of the Army, Office of the Deputy Chief of Staff, G-2 validates the DDL requirements, the specific content requirements contained in the DDL originate primarily with the organization that the authority is conveyed to. DDLs are living and evolving documents that reflect current requirements. As the Army or organization undergoes change, the enabling DDL must keep pace. For example, over the years, the Army has addressed readiness through efforts ranging from Army Force Generation to the Sustained Readiness Model to what is currently referred to as the Regionally Aligned Readiness and Modernization Model (known as ReARMM) process. Staffs take care at an organizational level to ensure that DDLs are not administratively prohibitive simply because they are out of date.

C-5. "The information can't be shared because we are not the proponent." While some truth rests in this justification, it does not become a hard no until the authority has formally denied coordination for permission to disclose. Recipients ensure that any justification offered to withhold permission is articulated to ensure the information proponent is also not operating from the position of a false no. Finally, as higher headquarters support is requested, it will need detailed information to make decisions for delegating disclosure.

Glossary

The glossary lists acronyms and terms with Army and joint definitions. The proponent publication for terms is listed in parentheses after the definition. This publication is not proponent for any terms.

SECTION I – ACRONYMS AND ABBREVIATIONS

A2D2	advanced affirmative disclosure determination
ABCANZ	American, British, Canadian, Australian, and New Zealand
AR	Army regulation
ATP	Army techniques publication
CUI	controlled unclassified information
DA	Department of the Army
DDL	delegation of disclosure authority letter
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODM	Department of Defense manual
FM	field manual
G-1	assistant chief of staff, personnel
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-4	assistant chief of staff, logistics
G-5	assistant chief of staff, plans
G-6	assistant chief of staff, signal
G-9	assistant chief of staff, civil affairs operations
JP	joint publication
MOE	measure of effectiveness
MOP	measure of performance
MPE	mission partner environment
MPN	mission partner network
NOFORN	not releasable to foreign nationals
S-1	battalion or brigade personnel staff officer
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
S-4	battalion or brigade logistics staff officer
S-5	battalion or brigade plans staff officer
S-6	battalion or brigade signal staff officer

S-9	battalion or brigade civil affairs operations staff officer
U.S.	United States
WFR	write for release

SECTION II – TERMS

constraint

(Army) A restriction placed on the command by a higher command. A constraint dictates an action or inaction, thus restricting the freedom of action of a subordinate commander. (FM 5-0)

distribution statement

A statement used to mark technical information to indicate the extent of its availability for secondary distribution, release, and disclosure without additional approvals or authorizations. A distribution statement marking is distinct from and in addition to a security classification marking assigned in accordance with Volume 2 of DODM 5200.01. (DODI 5230.24)

measure of effectiveness

An indicator used to measure a current system state, with change indicated by comparing multiple observations over time. (JP 5-0)

measure of performance

An indicator used to measure a friendly action that is tied to measuring task accomplishment. (JP 5-0)

mission partner

Partners with which the DoD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government, State and local governments, allies, coalition members, host nations and other nations, multinational organizations, non-governmental organizations, and the private sector. (DODD 5101.22E)

unified action partner

Those military forces, governmental and nongovernmental organizations, and elements of the private sector with whom United States Army forces plan, coordinate, synchronize, and integrate during the conduct of operations. Unified action partners include joint forces and components, multinational forces, and United States government agencies and departments. (AR 34-1)

References

All websites accessed on 14 June 2023.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. 15 August 2023.

FM 1-02.1. *Operational Terms*. 09 March 2021.

FM 1-02.2. *Military Symbols*. 18 May 2022.

RELATED PUBLICATIONS

These cited documents contain relevant supplemental information.

JOINT PUBLICATIONS

Most joint doctrinal and administrative publications are available online at https://www.jcs.mil/Doctrine/. Most Department of Defense publications are available at https://www.esd.whs.mil/dd/.

DODD 5101.22E. *DoD Executive Agent (DoD EA) for DoD Mission Partner Environment (MPE)*. 05 August 2020.

DODD 5230.11. *Disclosure of Classified Military Information to Foreign Governments and International Organizations*. 16 June 1992.

DODI 5230.24. *Distribution Statements on DOD Technical Information*. 10 January 2023.

DODI 5530.03. *International Agreements*. 4 December 2019.

DODM 5200.01. *DoD Information Security Program: Marking of Information*, Volume 2. 24 February 2012.

JP 5-0. *Joint Planning*. 01 December 2020.

(U) *National Disclosure Policy* (NDP-1). (This classified publication is available on the SIPRNET. Contact the preparing agency of this publication for access instructions.)

National Military Strategy. 2022. Available at https://www.jcs.mil/Portals/36/NMS%202022%20_%20Signed.pdf.

National Security Decision Memorandum 119. *Disclosure of Classified United States Military Information to Foreign Governments and International Organizations*. 20 July 1971. Available at https://www.nixonlibrary.gov/sites/default/files/virtuallibrary/documents/nsdm/nsdm_119.pdf.

National Security Strategy. December 2017. Available at https://www.hsdl.org/?abstract&did=806478.

ARMY PUBLICATIONS

Most Army doctrinal and administrative publications are available online at https://armypubs.army.mil/.

AR 34-1. *Interoperability*. 09 April 2020.

DA Pam 11-31. *Army Security Cooperation Handbook*. 06 February 2015.

FM 3-0. *Operations*. 01 October 2022.

FM 3-16. *The Army in Multinational Operations*. 08 April 2014.

FM 4-02. *Army Health System.* 17 November 2020.

FM 5-0. *Planning and Orders Production*. 16 May 2022.

FM 6-0. *Commander and Staff Organization and Operations*. 16 May 2022.

FM 6-27/MCTP 11-10C. *The Commander's Handbook on the Law of Land Warfare*. 07 August 2019.

ABCANZ PUBLICATIONS

Most ABCANZ publications are available online at https://www.apan.org/.

ABCANZ Publication 332. *Coalition Operations Handbook*, Edition 7. 15 September 2021.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, most Department of the Army (DA) forms are available on the Army Publishing Directorate website: https://armypubs.army.mil/.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

Index

Entries are by paragraph number.

Entries are by paragraph number.

ATP 3-16.02

26 September 2023

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army
2326208

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve. Distributed in electronic media only (EMO).

This page intentionally left blank.

PIN: 216177-000