



INSTITUTE FOR DEFENSE ANALYSES

Civilian Harm Mitigation and Response Action Plan (CHMR-AP): Objective 6 Results and Transition Plan

Laura A. Odell, Project Leader

Clifford M. Bridges

Cameron D. DiLorenzo

Claire E. Haas

Todd D. Sabala

Miranda G. Seitz-McLeese

August 2023

Distribution Statement A.
Approved for public release:
distribution is unlimited.

IDA Product 3000981

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305



The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project BC-5-4826, "Army Fusion Cell," for the HQDA OCIO. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For More Information

Laura A. Odell, Project Leader
lodell@ida.org, 703-845-2009/703-845-2009

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Copyright Notice

© 2023 Institute for Defense Analyses
730 East Glebe Road, Alexandria, Virginia 22305 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (Feb. 2014).

Rigorous Analysis | Trusted Expertise | Service to the Nation

Executive Summary

On August 25, 2022, the Department of Defense (DoD) released its Civilian Harm Mitigation and Response Action Plan (CHMR-AP) to improve strategic outcomes, optimize military operations, and strengthen DoD mitigation of civilian harm through a reinforcing framework. Objective 6 (OBJ 6) of the CHMR-AP tasks the Secretary of the Army (SECARMY) with developing a data management platform (DMP) for CHMR-related data.

This report documents OBJ 6 activities completed to date by the OBJ 6 Working Group, led by HQDA G-3/5/7.¹ The status of the activities is detailed in Table EX-1.

Table EX-1. OBJ 6 Actions and Status

OBJ 6 Actions and Status		
Phase 0 (FY22)	6.a: Joint Proponent leads development of a DMP.	Complete
	6.b: Joint Proponent lead provides an initial cost estimate associated with developing and fielding the DMP.	Complete
	6.c: Under Secretary of Defense for Policy (USD(P)) submits a FY23 Unfunded Requirement (UFR) that includes initial projected costs associated with the DMP.	Complete
	6.d: USD(P) presents draft DoD Instruction (DoDI) for CHMR to the Secretary of Defense (SECDEF).	Complete
Phase 1 (FY23)	6.e: USD(P) submits issue paper for the FY 24-28 President's Budget Request (PBR).	Complete
	6.f: Joint Proponent develops and refines more specific information requirements and data sources that will populate the DMP.	Complete
	6.g: Joint Proponent develops and refines more specific technical requirements of the DMP.	In Progress

¹ Appendix A provides details on Objective 6 Working Group members.

OBJ 6 Actions and Status		
	6.h: Joint Proponent selects from existing programs, develops its own DMP, or contracts for a DMP.	In Progress
	6.i: Joint Proponent refines cost estimates associated with the DMP.	To Be Completed
	6.j: Joint Staff and combatant commands establish standardized processes for reporting civilian harm.	To Be Completed
Phase 2 (FY24)	6.k: Joint Proponent submits a FY25 issue paper for enduring CHMR requirements.	To Be Completed
	6.l: Joint Proponent develops and distributes standard operating procedures for the DMP.	To Be Completed
	6.m: Joint Proponent develops and provides training across the joint force.	To Be Completed
Phase 3 (FY25)	6.n: Combatant commands and other relevant DoD and Office of the Secretary of Defense (OSD) components employ the data management tool as the authoritative platform for the collection of CHMR reporting and data management.	To Be Completed

The Civilian Protection Center of Excellence (CP CoE) and the Data and Analytics Response Team (DART) are the recommended champions for the remaining Phase 1–3 OBJ 6 activities — the CP CoE, as the lead for DMP decision making, management, and sustainment, and the DART as the technical support provider, focusing on technical requirements and on building a minimally viable product (MVP). All transition activities appear in Table EX-2 and are aligned with the recommended lead.

Table EX-2. Summary of Proposed Transition Actions

CHMR-AP Phase	CHMR-AP Action	Proposed Lead	Proposed Transition Actions
Phase 1 (FY23)	6.f	CP CoE	Conduct data call to identify data system points of contact.
	6.g	CP CoE	Manage refinements to DMP information requirements and data sources as CHMR roles and processes mature.
	6.g	DART	Align information requirements (see Appendix D) to data sources (see Appendix E) via data requirements.

CHMR-AP Phase	CHMR-AP Action	Proposed Lead	Proposed Transition Actions
	6.g	DART	Engage the CHMR community of interest to develop and refine DMP technical requirements.
	6.g	DART	Leverage information requirements, data requirements, and data sources to prioritize technical requirements for MVP.
	6.h	CP CoE & DART	Identify candidate platforms, including existing platforms and a development option, for analysis of alternatives (AoA).
	6.h	CP CoE & DART	Perform an AoA to select a platform that meets DMP evaluation criteria—focusing on technical requirements at the MVP stage—and can scale to meet DMP needs once the platform reaches FOC.
	6.i	CP CoE	Refine DMP cost estimates to include considerations related to platform selection, MVP development, and sustainment as the DMP progresses toward FOC.
	6.j	CP CoE	Coordinate with Joint Staff and combatant commands (CCMDs) to ensure the DMP supports any standardized processes developed.
Phase 2 (FY24)	6.l, 6.n	CP CoE	Develop and distribute DMP standard operating procedures (SOPs). Coordinate with the DMP developer to create and provide training to data managers and units as appropriate.
Phase 3 (FY25)	6.n	CP CoE	Coordinate with DMP users to support standard utilization of the DMP by those with the same roles. Brief the CHMR Steering Committee on CCMD DMP adoption.

Completion of OBJ 6 tasks is necessary to execute and standardize across the CHMR effort. Objective leads support the tasks outlined in the strategic roadmap (see Figure EX-1), closely coordinating and addressing potential disconnects as operating constructs are finalized. This roadmap identifies immediate and long-term tasks needed to achieve platform FOC, thereby aligning actions to outcomes consistent with the CHMR-AP.

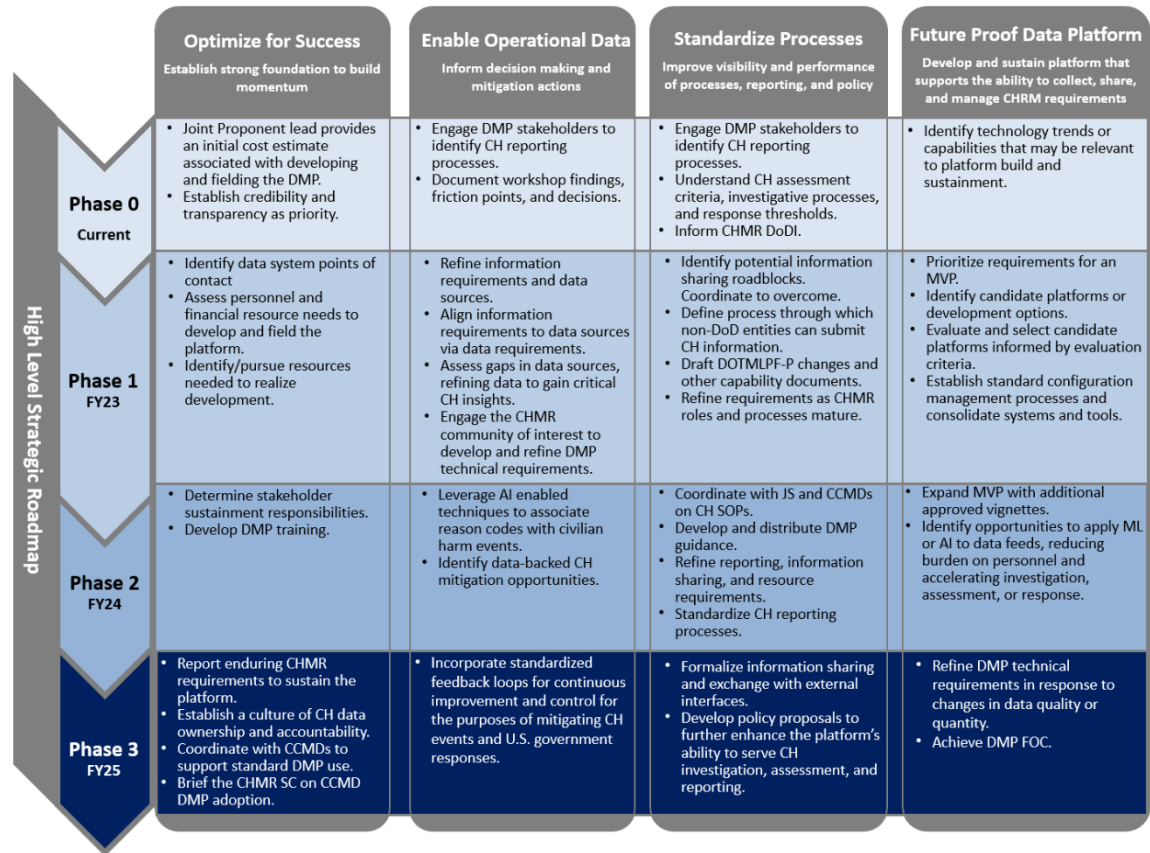


Figure EX-1. DMP Strategic Roadmap

Contents

1.	CHMR-AP Objective 6	1-1
A.	Introduction	1-1
B.	Report Focus.....	1-3
2.	CHMR-AP Objective 6 Background.....	2-1
A.	Defining Data Management and a DMP	2-1
B.	CHMR-AP Scoping and Assumptions	2-2
C.	DMP Scoping and Assumptions.....	2-3
1.	Consideration: Data Management Roles and Responsibilities.....	2-5
D.	OBJ 6 Status, Dependencies, and Actions	2-6
3.	Phase 0 (FY22) Activities and Results.....	3-8
4.	Phase 1 (FY23) Activities and Results.....	4-1
A.	Overview of Phase 1.....	4-1
B.	Action 6.f.....	4-2
1.	Vignettes and Key Users	4-3
2.	Information Requirements and Potential Data Sources	4-4
C.	Action 6.g	4-6
1.	Consideration: Prioritizing for an MVP	4-8
D.	Action 6.h	4-11
1.	Considerations: Platform Evaluation Criteria	4-12
E.	Action 6.i.....	4-14
F.	Action 6.j.....	4-15
5.	Phase 2 (FY24) and Phase 3 (FY25) Considerations	5-1
A.	Phase 2 (FY24) Considerations.....	5-1
B.	Phase 3 (FY25) Considerations.....	5-1
6.	Summary of Transition Actions	6-1
	Appendix A. CHMR Policy Background	A-1
	Appendix B. OBJ 6 Working Group Members	B-1
	Appendix C. Vignettes.....	C-1
	Appendix D. Detailed Information Requirements	D-1
	Appendix E. Data Sources	E-1
	Appendix F. Dependency Analysis.....	F-1
	Appendix G. CHMR OBJ 6 Technical Exchange Meeting Proceedings.....	G-1

Figures and Tables

Figure EX-1. DMP Strategic Roadmap	iv
Figure 2-1. Data Life Cycle	2-1
Figure 2-2. Scoping per CHMR-AP & Draft DoDI 3000.LT.....	2-3
Figure 2-3. DMP Expectations	2-5
Figure 2-4. OBJ 6 Actions and Status.....	2-6
Figure 2-5. OBJ 6 Actions and Phases.....	2-7
Figure 4-1. Generalized Vignette Process Flow and Core DMP Uses	4-2
Figure 4-2. Example MVP Prioritizing CCMD, IO, and CP CoE Users, Automated Reporting, and Activity Recording.....	4-10
Figure 4-3. Example MVP1 Maturation and Build Out	4-11
Figure 6-1. DMP Strategic Roadmap.....	6-2
Figure C-1. Vignettes and DMP Use Cases.....	C-1
Figure C-2. Targeting Process & DMP Overlay.....	C-2
Figure C-3. Troops In Contact Process & DMP Overlay	C-2
Figure C-4. False Claim Process & DMP Overlay	C-3
Figure C-5. Sensitive Activities Process & DMP Overlay	C-4
Figure C-6. Sensitive Activities Process & DMP Overlay	C-4
Figure F-1. Input Coordinators by Action Count.....	F-4
Figure F-2. Input Distribution by Phase	F-5
Figure F-3. Output Coordinators by Action Count.....	F-7
Figure F-4. Output Distribution by Phase.....	F-8
Table EX-1. OBJ 6 Actions and Status.....	i
Table EX-2. Summary of Proposed Transition Actions	ii
Table 1-1. CHMR OBJs.....	1-1
Table 1-2. OBJ 6 Actions and Status	1-2
Table 4-1. Vignettes and Characteristics	4-3
Table 4-2. Vignettes and Key Users	4-4
Table 4-3. CCMD Information Requirements within Targeting Vignette	4-4
Table 4-4. Count of In-Scope Data Systems by Vignette.....	4-5
Table 4-5. Count of In-Scope Data Systems by Component.....	4-5
Table 4-6. Sample Information Requirements and Data Requirements with Notional Technical Requirements	4-7
Table 6-1. Summary of Proposed Transition Actions	6-1
Table A-1. Federal-level Policies on Civilian Harm Due to U.S. Military Operations..	A-1
Table A-2. Service-level Policies on Civilian Harm	A-3
Table B-1. OBJ 6 Working Group Participants.....	B-1

Table D-1. Detailed Information Requirements by Vignette and Key User.....	D-1
Table E-1. Data Systems In Scope for DMP	E-1
Table E-2. Data Systems Requiring Additional Research to Determine DMP Relevance.....	E-31
Table F-1. Interdependency Counts by Objective & Dependency	F-2
Table F-2. Inputs by Objective & Type	F-3
Table F-3. Inputs by Objective & Phase	F-5
Table F-4. Outputs by Objective & Type	F-6
Table F-5. Outputs by Objective & Phase	F-7

1. CHMR-AP Objective 6

A. Introduction

On August 25, 2022, the Department of Defense (DoD) released its Civilian Harm Mitigation and Response Action Plan (CHMR-AP). The plan, directed by the Secretary of Defense, creates new institutions and processes that will improve strategic outcomes, optimize military operations, and strengthen DoD's ability to mitigate civilian harm during operations through a reinforcing framework. The CHMR-AP designates the Secretary of the Army (SECARMY) as the Executive Agent and Joint Proponent for CHMR. It also creates the following CHMR-focused organizational elements: the Civilian Protection Center of Excellence (CP CoE), as a home for CHMR analysis, learning, and training; Civilian Environment Teams, which illuminate the civilian environment for commanders; Civilian Harm Assessment Cells (CHACs), which assess civilian harm (CH) resulting from operations; and CHMR Officers (CHMROs), which convene working groups to ensure CHMR activities are integrated into command efforts.

The Action Plan is made up of 11 Objectives (OBJs), each with subordinate actions, sequenced in phases that align with fiscal years (FY). Table 1-1 shows each OBJ and a brief thematic summary.

Table 1-1. CHMR OBJs

OBJ
OBJ 1: Establish CHMR Steering Committee
OBJ 2: Establish CP CoE
OBJ 3: Institutionalize CHMR Guidance
OBJ 4: Integrate CHMR into Joint Targeting
OBJ 5: Improve Positive Identification
OBJ 6: Develop CH Data Management Processes
OBJ 7: Establish Department-Wide CH Procedures
OBJ 8: Refresh DoD CH Guidance
OBJ 9: Integrate CHMR into Security Cooperation
OBJ 10: Refresh Multinational CH Guidance

OBJ
OBJ 11: Resource CHMR

CHMR-AP OBJ 6 is tasked to the SECARMY to develop a data management platform (DMP) to enable civilian harm data harmonization, analytics, and decision support. This effort seeks to improve how DoD collects, shares, and gains insight from data related to civilian harm. There are 14 actions included under OBJ 6 (6.a through 6.n) that drive DMP development and integration into CHMR processes. The actions in Table 1-2 are spread across FY22 through FY25.

Table 1-2. OBJ 6 Actions and Status

OBJ 6 Actions and Status		
Phase 0 (FY22)	6.a: Joint Proponent leads development of a DMP.	Complete
	6.b: Joint Proponent lead provides an initial cost estimate associated with developing and fielding the DMP.	Complete
	6.c: Under Secretary of Defense for Policy (USD(P)) submits a FY23 Unfunded Requirement (UFR) that includes initial projected costs associated with the DMP.	Complete
	6.d: USD(P) presents draft DoD Instruction (DoDI) on CHMR to the Secretary of Defense (SECDEF).	Complete
Phase 1 (FY23)	6.e: USD(P) submits issue paper for the FY 24-28 President's Budget Request (PBR).	Complete
	6.f: Joint Proponent develops and refines more specific information requirements and data sources that will populate the DMP.	Complete
	6.g: Joint Proponent develops and refines more specific technical requirements of the DMP.	In Progress
	6.h: Joint Proponent selects from existing programs, develops its own DMP, or contracts for a DMP.	In Progress
	6.i: Joint Proponent refines cost estimates associated with the DMP.	To Be Completed
	6.j: Joint Staff and combatant commands establish standardized processes for reporting CH.	To Be Completed

OBJ 6 Actions and Status		
Phase 2 (FY24)	6.k: Joint Proponent submits a FY25 issue paper for enduring CHMR requirements.	To Be Completed
	6.l: Joint Proponent develops and distributes standard operating procedures for the DMP.	To Be Completed
	6.m: Joint Proponent develops and provides training across the joint force.	To Be Completed
Phase 3 (FY25)	6.n: Combatant commands and other relevant DoD and Office of the Secretary of Defense (OSD) components employ the data management tool as the authoritative platform for the collection of CHMR reporting and data management.	To Be Completed

All FY22 activities are complete. FY23 activities are ongoing. FY24 and FY25 activities depend upon the completion of FY23 activities.

B. Report Focus

This report documents OBJ 6 activities completed to date by the OBJ 6 Working Group, led by SECARMY as the CHMR Executive Agent.² The report focuses on the results of completed FY22 and FY23 activities and a transition plan for remaining FY23 activities. The CP CoE and Data and Analytics Response Team (DART) are the recommended champions for the remaining OBJ 6 activities — the CP CoE, as the lead for DMP decision making, management, and sustainment and the DART as the technical support provider, focusing on technical requirements and on building a minimally viable product (MVP). The DART team will conduct a six month sprint activity and then transition results to the CP CoE. Recommended transition activities are assigned to one of these two entities throughout the report. The report is structured as follows:

- Section 2 provides background information on data management, DMP scoping considerations, and OBJ 6 dependencies.
- Section 3 details Phase 0 (FY22) results.
- Section 4 details Phase 1 (FY23) results, ongoing work, and transition considerations.

² Appendix B provides details on OBJ 6 Working Group members.

- Section 5 provides Phase 2 (FY24) and Phase 3 (FY25) considerations.
- Section 6 provides a summary of all recommended transition actions.

2. CHMR-AP Objective 6 Background

A. Defining Data Management and a DMP

Successful high-performing public and private businesses derive value from their data. In its 2020 Data Strategy, the DoD noted that leveraging data as a strategic asset requires that data be visible, accessible, understandable, linked, trustworthy, interoperable, and secure.³ It can be difficult to ensure data meets these objectives throughout the data life cycle (see Figure 2-1) as data sources, users, use cases, and business needs grow. A DMP is a system designed to simplify data management throughout the life cycle of data.

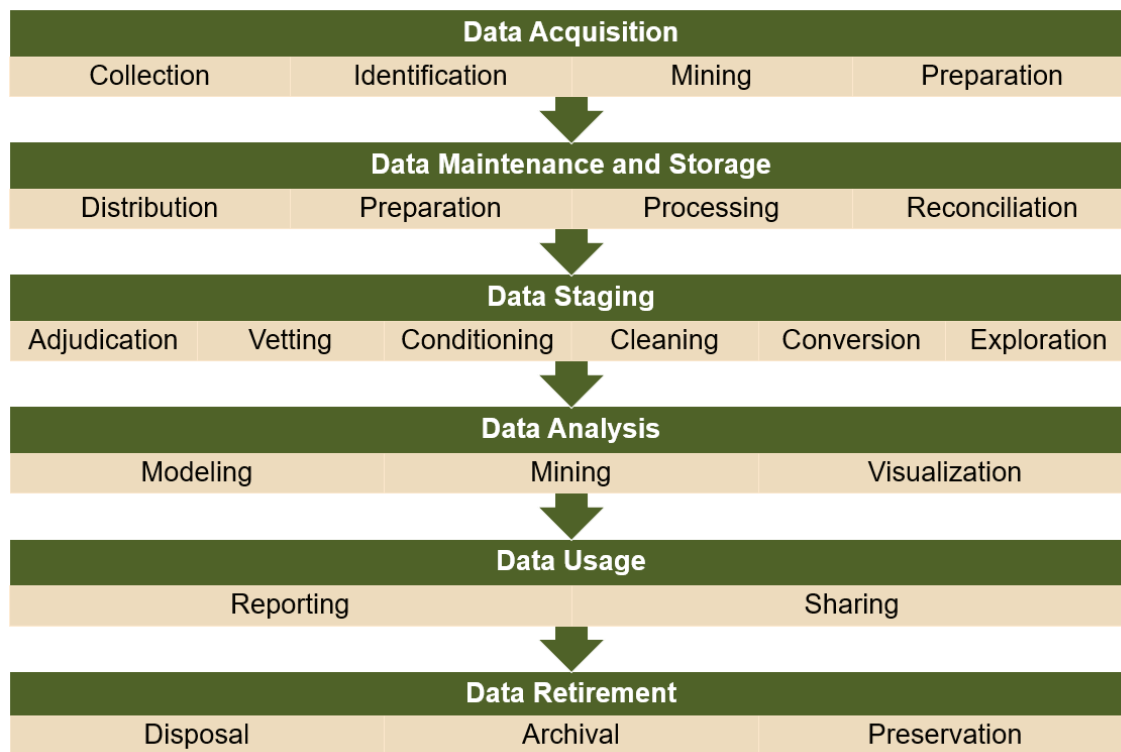


Figure 2-1. Data Life Cycle

A DMP provides a centralized interface for disparate data sources and supports the entire data life cycle by merging, analyzing, and reporting select data. Extensibility and auditability are key DMP properties. Extensibility allows a DMP to ingest and integrate new data into the platform via data pipelines as new data sources emerge. An extensible

³ See the 2020 DoD Data Strategy for further discussion on making data a strategic asset:
<https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>

DMP also supports including new analytical components and capabilities into the platform, allowing it to remain relevant and valuable through fast-changing mission needs. Auditability supports DMP management by tracking access for overall security management, tracking workflows of deliverables as needed, and ensuring the platform's overall performance. Within the DoD, auditability also includes meeting data strategy objectives.⁴

DMP functionality depends on the intended users, information requirements, and use cases for the underlying data. As with all datasets, a DMP without well-defined use cases or information requirements likely provides little value to its users. Ingesting, merging, analyzing, and reporting data within the DMP may or may not be automated. Any automation requirements should be determined by the intended user base and their needs. However, any software tools needed to perform these functions should be contained within and be compatible with the DMP.

B. CHMR-AP Scoping and Assumptions

The CHMR-AP and the draft DoDI 3000.LT establish parameters for DoD CHMR efforts. Per the draft DoDI, CHMR efforts only apply to military operations during the conduct of hostilities. The OBJ 6 Working Group considers the following out of scope: training accidents, humanitarian assistance or disaster relief, and civilian casualties (CIVCAS) resulting from foreign use of U.S. military equipment. A civilian harm incident also exceeds the scope of CHMR efforts if credible information emerges that civilian harm resulted from criminal activity.⁵ Multinational military operations are covered, and the draft DoDI instructs CCMDs to coordinate with allies and partners to establish shared guidance and processes to assess CH. In addition, the draft DoDI focuses on acknowledgements and condolence payments (e.g., *ex gratia*) as responses to CH. In contrast, casualty evacuations and humanitarian aid are outside the scope of the CHMR-AP and the draft DoDI. Figure 2-2 depicts these high-level scoping parameters.

⁴ See the 2020 DoD Data Strategy: <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>

⁵ Draft DoDI 3000.LT, 4.5.e(2)

CH Scope: Military operations during the conduct of hostilities.

- Out: Training accidents, HADR, CIVCAS from foreign use of U.S. equipment
- Out: Criminal activity

Response Scope: U.S. Government CH responses.

- In: Acknowledgement, Condolence Payments
- Out: CASEVAC, Humanitarian Aid

Role of the CCMD/CCDR:

- Determine whether, how, and when to respond to CH.
- Establishes operation-specific guidance for CH assessments/investigations.
- May delegate authority to initiate/approve CH to a designee under their command.
- Coordinates with allies/partners to establish shared guidance to respond to CH resulting from multinational operations.

Role of the CHACs (subordinate to CCMDs)

- Receive and compile CH information.
- Coordinate with investigators when practical.

Figure 2-2. Scoping per CHMR-AP & Draft DoDI 3000.LT

The draft DoDI highlights the role of the Combatant Commander (CCDR) in assessing, investigating, and responding to CH. The draft DoDI states that the CCDR determines whether, how, and when to respond to CH.⁶ CCDRs also establish operation-specific guidance for civilian harm assessments and investigations⁷ and may delegate authority to initiate or approve civilian harm assessments to a designee under their command.⁸ The draft DoDI specifies that the document does not limit CCDR authorities to “initiate an investigation or other administrative proceedings related to civilian harm or other matters.”⁹ The draft DoDI clarifies the role of the CHACs, stating that they are subordinate to CCMDs, that they receive and compile civilian harm information, and that they should coordinate with CH investigators when practical.¹⁰ A detailed CHMR policy review is provided in Appendix A.

C. DMP Scoping and Assumptions

The CHMR-AP states that the DMP should consider interoperability with allies and partners, support data related to multinational operations, and include a mechanism for

⁶ Draft DoDI 3000.LT, 5.2.f

⁷ Draft DoDI 3000.LT, 2.16.n

⁸ Draft DoDI 3000.LT, 4.2.g(2)(b)

⁹ Draft DoDI 3000.LT, 4.6.f.

¹⁰ Draft DoDI 3000.LT, 4.3

members of the public and non-DoD entities to submit CH information for consideration.¹¹ DMP users will need access to summary data on the totality of military operations. This data places the number of CH incidents in context, showing effectiveness of CH countermeasures in all missions, not simply the missions resulting in CH. The draft DoDI states the DMP should include, “at a minimum,”¹² the following CH related data: operation date and location; operation type; “amplifying” operational details (e.g., direct versus indirect fire, deliberate versus dynamic targeting); participating units and platforms; and results of reviews, assessments, or investigations.

These requirements have implications for DMP functionality, which are shown in Figure 2-3. The DMP should be able to accept reports from disparate sources; manage data at different stages of the data life cycle; support data collection, retention, and analysis; enable data analytics; and record CH assessment and investigation results or responses. The requirements described in the CHMR-AP and draft DoDI 3000.LT also have implications for what expectations are not placed on the DMP. For example, the DMP is not expected to replace human-on-the-loop activities, such as vetting and adjudicating information. The DMP also does not replace targeting processes or targeting systems. Rather, it draws on these systems as feeds. Finally, the DMP does not replace the investigation process, nor does it alter existing records management requirements. Given this, DMP functionality aligns more to that of a business system than that of a national security system.

¹¹ Action 6.f, <https://media.defense.gov/2022/Aug/25/2003064740/-1/-1/1/CIVILIAN-HARM-MITIGATION-AND-RESPONSE-ACTION-PLAN.PDF>

¹² Draft DoDI 3000.LT, 4.7.(b)

**IN**

- Accepts reports from disparate sources.
- Considers interoperability with Allies and Partners.
- Supports data related to multi-domain US operations, multi-national operations, and operations with non-state actors.
- Includes a mechanism for members of the public and other non-DoD entities to submit civilian harm information for consideration.
- Supports the collection, appropriate retention, and analysis of information.
- Manages data at different stages of data lifecycle
- Enables data analytics
- Records results

OUT

- Does not replace the human-on-the-loop (i.e., vetting and adjudication).
- Does not replace the targeting process or targeting systems.
- Does not replace the investigation process or records management requirements.

Figure 2-3. DMP Expectations

1. Consideration: Data Management Roles and Responsibilities

Per leadership direction, the CP CoE will be responsible for platform sustainment, including DMP provisioning, development, sustainment, and security. The CP CoE will need to interact frequently with the DMP user base to ensure the platform meets need. Additional considerations include the following:

- **Provisioning:** The provisioning team will assess available platforms, including a possible new platform built specifically for the DMP, and select one. Once compute and store are available, the provisioning team can work to develop the workflow that best supports CHMR. To provide a capability that will best meet mission requirements, the team must consider access mechanisms, operation of role-based access control (RBAC), expected data retention periods, and any requirements to standardize reporting across CCMDs.
- **Development:** It is challenging to develop applications, data storage and archival systems, and analytics that incorporate information on both missions that result in CH and those that do not. Developers will likely require frequent communication with the user base in the initial stages and as the CHMR workforce continues to develop its understanding of how best to accomplish its roles and responsibilities.
- **Sustainment:** Early decisions regarding DMP operating systems, access mechanisms, and technology stack can be difficult to change. As such, DMP sustainers should be consulted during MVP development. Understanding the

sustainer’s skills, familiarity with technologies, and any architecture currently maintained can inform decisions that reduce training requirements and lower operating costs over the life of the DMP.

- **Security:** Security should be built into new platforms and capabilities. The sensitive nature of CH incidents may make the DMP a target for malicious actors. Secret networks provide some additional security over unclassified networks, but other measures would also be needed. For example, DMP RBAC could facilitate access management regardless of platform classification. RBAC may include developer, operator, sustainer, and user roles, with some roles (e.g., CCMDs, CP CoE) having broad access to CH incident data and other roles having narrower access. Encrypting data at rest may mitigate the risk of any retained sensitive data. Early identification of a Cyber Security Service Provider may also contribute to DMP security, as that organization’s standard capabilities for defense and log aggregation could be considered for integration within the DMP.

D. OBJ 6 Status, Dependencies, and Actions

Some OBJ 6 actions have already been completed, while others remain in progress. Figure 2-4 displays the status of each action thus far.

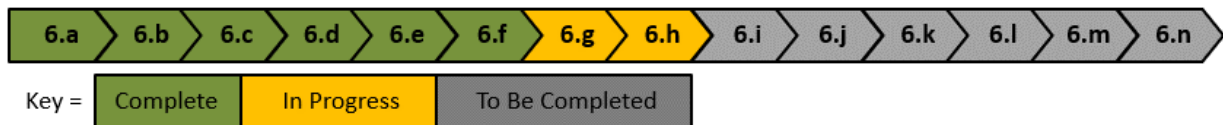


Figure 2-4. OBJ 6 Actions and Status

The OBJ 6 Working Group performed an interdependency analysis to identify activities and data outside OBJ 6 that inform the DMP (i.e., inputs). This includes activities and data that generate standards or information other OBJs will need to leverage (i.e., outputs). This interdependency analysis is included as Appendix F. Although some inputs or outputs may inform (or be informed) by the DMP, no dependencies prevent DMP development. The only true dependencies for the DMP exist within OBJ 6 itself. Figure 2-5 depicts all CHMR-AP OBJ 6 actions by type and scheduled phase.

CHMR-AP OBJ6 Actions						
System Action 		Resourcing Action 	Policy Action 	Training Action 		
Objective	Action	Action Details	FY22	FY23	FY24	FY25
6	6.a.	Designate SECARMY as CHMR DMP lead.				
	6.b.	Initial cost estimate for development & fielding. Provide to CHMR SC.				
	6.c.	Coordinate submission of FY23 UFR covering initial CP CoE and CHMR costs.				
	6.d.	Coordinate with USD(P) to ensure CHMR DoDI establishes responsibilities for developing an..				
	6.e.	Coordinate submission of FY24-FY28 Program and Budget Review issue paper.				
	6.f.	Develop and refine information requirements and data sources.				
	6.g.	Develop and refine data management platform technical requirements.				
	6.h.	Develop DOTMLPF-P change recommendation and other capability documents for validation.				
		Select data management platform meeting technical and information requirements.				
	6.i.	Refine cost estimates and provide to CHMR SC.				
	6.j.	Coordinate on Joint Staff/CCMD establishment of standardize processes for reporting CH.				
	6.k.	Develop legislative proposals.				
		Submit FY25 Issue Paper for enduring CHMR requirements.				
	6.l.	Develop and distribute data management system SOPs.				
	6.m.	Coordinate with platform developer and CP CoE to develop and provide user training.				
	6.n.	Fully Operational Capability.				

Figure 2-5. OBJ 6 Actions and Phases

Actions 6.f, 6.g, 6.h, and 6.i are dependent upon each other, and these must proceed in order. Action 6.f tasks the CHMR Joint Proponent with developing and refining DMP information requirements and data sources. This action also prescribes including certain categories of data into the DMP and providing a public access mechanism for submitting CH information. Action 6.g prescribes developing DMP technical requirements, which should follow from and speak to information requirements. These technical requirements then drive platform selection (or development) discussed in 6.h. Action 6.i calls for refined DMP cost estimates, which are driven by the platform selection taking place in 6.h. Given the impact each of these actions has on subsequent actions, they must be performed serially.

It is important to note that, from a personnel perspective, the DART requires certain conditions for its involvement. Namely, the DART cannot undertake its six month sprint activity supporting Action 6.g unless those involved in DMP sustainment within the CP CoE have been hired and are in place. Consideration: Data Management Roles and Responsibilities

3. Phase 0 (FY22) Activities and Results

Phase 0 establishes roles and responsibilities with respect to DMP development, initial cost estimates, and supporting policies. The following actions took place in Phase 0:

- 6.a: Joint Proponent leads development of a DMP.
- 6.b: Joint Proponent provides an initial cost estimate considering DMP development and fielding.
- 6.c: USD(P) submits a FY23 UFR including initial projected costs associated with the DMP.
- 6.d: USD(P) presents a draft DoDI on CHMR to SECDEF.

All Phase 0 actions have been completed. Initial cost estimates developed in support of 6.b and in support of Phase 1 action 6.e prescribes a dollar amount per fiscal year across the future years defense program (FYDP).¹³ Though Action 6.c calls for submitting a UFR, none was submitted, as the CHMR-AP was included in FY23 appropriation. The draft DoDI on CHMR remains with the DoD Office of General Counsel as of July 31, 2023.

¹³ <https://armyetaas.sharepoint-mil.us/teams/CHMR-APOBJ6/Shared%20Documents/Forms/AllItems.aspx?id=%2Fteams%2FCHMR%2DAPOBJ6%2FShared%20Documents%2FGeneral%2F20220812%20%28CUI%29%20USD%2DP%20CHMR%20Issue%20Paper%2Epdf&parent=%2Fteams%2FCHMR%2DAPOBJ6%2FShared%20Documents%2FGeneral>

4. Phase 1 (FY23) Activities and Results

A. Overview of Phase 1

Phase 1 focuses on DMP development and prescribes defining critical information requirements, identifying data sources, developing DMP technical requirements, and selecting a platform. Phase 1 also prescribes refining cost estimates accordingly. The following actions are scheduled to take place in Phase 1:

- 6.e: USD(P) submits issue paper for the FY 24-28 President's Budget Request (PBR).
- 6.f: Joint Proponent develops and refines more specific information requirements and data sources that will populate the DMP.
- 6.g: Joint Proponent develops and refines more specific technical requirements of the DMP.
- 6.h: Joint Proponent selects from existing programs, develops its own DMP, or contracts for a DMP.
- 6.i: Joint Proponent refines cost estimates associated with the DMP.
- 6.j: Joint Staff and combatant commands establish standardized processes for reporting CH.

It will take multiple years of consistent effort to provide the comprehensive digital capability necessary to best support the community of interest. An incremental approach to digital support will provide initial capability and allow CHMR processes to mature, further defining the full functionality of the DMP.

Conceptual system requirements and system definition follow the below path:

- Identification of key users;
- Identification of key user information requirements;
- Identification of information systems which can provide necessary data;
- Evaluation and selection of a platform provider (e.g., buy or build).

CHMR is an ongoing effort to identify personnel, assign work roles, and develop appropriate processes. The concurrent development of a supporting DMP must be an iterative process. Decisions made for the initial DMP should enable the platform to support select CHMR users and also support the enduring solution without major modification.

B. Action 6.f

CHMR-AP 6.f: The joint proponent for CHMR, in coordination with DoD CIO, USD(A&S), USD(P), Joint Staff, combatant commands, the CP CoE, and other relevant DoD and OSD components, and with consideration for interoperability with allies and partners, develops and refines more specific information requirements and data sources that will populate the data management platform. This platform will incorporate information regarding U.S. operations, multinational operations, and operations with non-state actors. It will include a mechanism for members of the public and other non-DoD entities to submit for consideration information regarding civilian harm. It will also support the collection, maintenance, and analysis of information including, but not limited to, the following areas:

- i. Information indicating that civilian harm may have occurred including, where appropriate, open-source and other publicly available information
- ii. Operational data, regardless of whether information currently exists about whether civilian harm may have occurred, required to inform civilian harm assessments, including data from Mission Command Systems as described in

To identify information requirements consistent with Action 6.f, the OBJ 6 Working Group conducted a Technical Exchange Meeting (TEM) and leveraged five vignettes with a DMP functional overlay.¹⁴ These vignettes depict how key users may interact with the DMP. All vignettes follow a similar process flow, depicted by the green nodes in Figure 4-1. This generalized process flow can be customized to portray vignette-specific details. Blue cells show where the DMP intersects the process flow to perform the following core functions: ingest, conditioning, recording, automation, and data analytics.

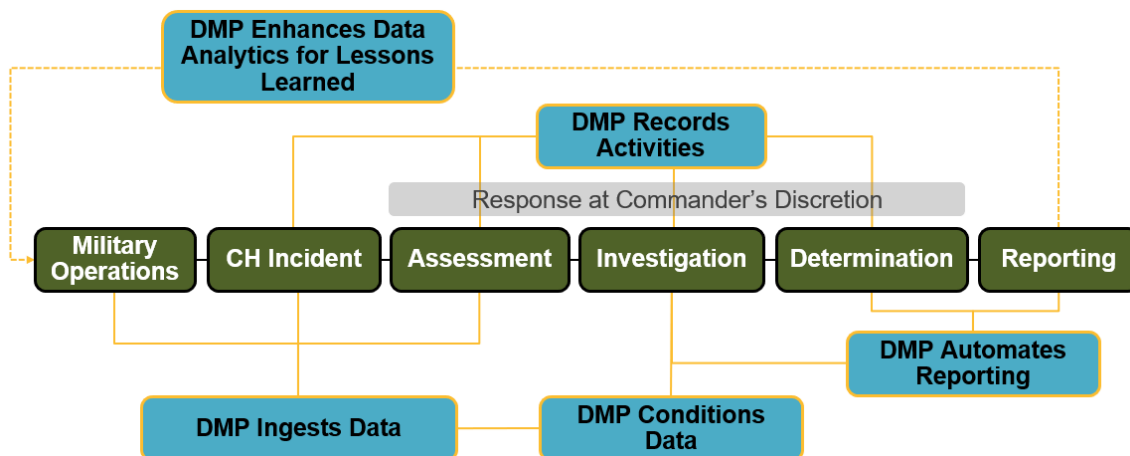


Figure 4-1. Generalized Vignette Process Flow and Core DMP Uses

¹⁴ TEM proceedings are included in Appendix G.

1. Vignettes and Key Users

The IDA team developed the following vignettes: Targeting, Sensitive Activities (e.g., Cyber Operation), False Claim, Multinational Operation, and Troops in Contact. Vignettes varied by CCMD, engagement type, response, responsibility, and submission mechanism. Table 4-1 illustrates the different elements present in each vignette.

Table 4-1. Vignettes and Characteristics

Vignette	CCMD	Engagement	Response	Responsibility Determination	Submission Mechanism
Targeting	AFRICOM	Kinetic	Ex Gratia	Affirmative	News/NGO
Troops in Contact	CENTCOM	Kinetic	Ex Gratia	Affirmative	Self-Report
False Claim	CENTCOM	None	Public Report	Negative	Public Access
Multinational Operation	PACOM	Kinetic	Ex Gratia	Negative	Public Access
Sensitive Activities	CYBERCOM	Non-Kinetic	None	Affirmative	News

Each vignette includes key users that perform certain actions and interact with the DMP. The following key users were identified:

- The Civilian Protection Center of Excellence (CP CoE)
- CCMD CH Personnel (e.g., CHACs, CHMROs)
- Investigating Officer (IO)
- Civil Affairs (CA) personnel
- The Public (P)
- Others (e.g., Allies and Partners)

Table 4-2 depicts how these users are present across the vignettes. Appendix C details the vignettes, where bracketed abbreviations indicate key user actions.

Table 4-2. Vignettes and Key Users

User	Targeting	Troops In Contact	False Claim	Multinational Operation	Sensitive Activities
CCMD	✓	✓	✓	✓	✓
IO	✓	✓	✓	✓	✓
CP CoE	✓	✗	✗	✓	✗
CA	✗	✗	✓	✓	✗
P	✗	✗	✓	✓	✗
Others	✗	✗	✗	✓	✗

2. Information Requirements and Potential Data Sources

Information requirements address what DMP users require from the platform. Each key user has information requirements that follow from their actions in the context of a particular vignette. For example, to produce and disseminate standardized CH reporting, users require the DMP to access investigation and CH assessment metadata, generate and report summary statistics about CH incidents, and generate standardized reporting elements at various classification levels. The OBJ6 Working Group held a TEM to identify the information requirements across all of the vignettes. Table 4-3 shows example information requirements for the CCMD user role within the Targeting vignette. Appendix D contains completed information requirements for each key user organized by vignette.

Table 4-3. CCMD Information Requirements within Targeting Vignette

Vignette	Key User	User Action	Information Requirement
Targeting	CCMD	Perform CH assessment.	Create a CH assessment file, connecting to meta-data for inclusion as appropriate.
Targeting	CCMD	Record CIVCAS allegation.	Create an investigation/allegation file, connecting to meta-data for inclusion as appropriate.
Targeting	CCMD	Support CCMD response to CH incident.	Record findings and response, storing investigation-relevant data as appropriate.

Information requirements also connect to data sources, via data requirements. These sources, which may be information repositories or platforms combining other feeds, contain the data objects and data elements on which the DMP should act to meet

information requirements. IDA was provided a list of approximately 3,600 DoD data systems documented by the DoD Chief Information Officer (CIO) DoD Information Technology Portfolio Repository (DITPR). The IDA team triaged these systems to prioritize those that contained operational or intelligence information, as well as the existing data platforms that aggregate data from a variety of systems. Appendix E contains the list of 214 systems found to be in scope for the DMP aligned to the vignettes.¹⁵ Table 4-4 depicts the distribution of those systems that are in scope across vignettes, with a majority (125) aligning to the Targeting vignette.

Table 4-4. Count of In-Scope Data Systems by Vignette

Metric	Targeting	Troops in Contact	False Claim	Multinational Operation	Sensitive Activities
Data System Count	125	96	121	104	62

Table 4-5 breaks down the in-scope data systems by component. These entities have information on system architecture, data objects, and any interconnections with other systems. These details may inform what sources are candidates for DMP inclusion.

Table 4-5. Count of In-Scope Data Systems by Component

Entity	Army	ASD(PA)	CDAO	DA&M	DISA	DIA	DLA
Data System Count	70	1	3	1	10	3	5
Entity	DON/Navy	DSCA	DTRA	Joint Staff	MDA	NSA	USAF
Data System Count	29	3	1	4	1	1	38
Entity	CENTCOM	USD(I)	USD(P&R)	INCOPACOM	USMC	STRATCOM	TRANSCOM
Data System Count	8	1	1	1	25	1	7

¹⁵ An additional 226 systems may be in scope for the DMP but require further research. These are also noted in Appendix E.

Proposed Transition Action 1: Adopt a data call to identify data system points of contact. (CP CoE)

As CHMR roles and processes mature, additional information requirements will be identified that may drive refinement.

Proposed Transition Action 2: Manage refinements to DMP information requirements and data sources as CHMR roles and processes mature. (CP CoE)

C. Action 6.g

CHMR-AP 6.g: *The joint proponent for CHMR, in coordination with USD(A&S), DoD CIO, and Joint Staff, develops and refines more specific technical requirements of the data management platform.*

Technical requirements are specifications for infrastructure, open architecture, data standards, data management, hosting and security, and life-cycle support requirements (e.g., availability, scalability, maintainability, supportability, and interoperability).¹⁶ Technical requirements are informed by the information requirements generated in 6.f.

Given information requirements, one can derive data requirements that support the information needed, identify data sources providing the data requirements, and develop technical requirements to manage the data and data sources. Table 4-6 provides a sample of aligning information requirements to technical requirements by identifying data requirements in the DMP context. To develop and refine technical requirements for the DMP, one should first derive data requirements from information requirements and align those to the data sources provided in Appendix E.

Proposed Transition Action 3: Align information requirements (see Appendix D) to data sources (see Appendix E) via data requirements. (DART)

¹⁶ DoDI 5000.75, Business Systems Requirements and Acquisition,
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500075p.PDF>

Table 4-6. Sample Information Requirements and Data Requirements with Notional Technical Requirements

User	Information Requirement	Data Requirement	Technical Requirements
CCMD	Identify trends in CH in the past year within area of responsibility (AOR).	Count of all (deduplicated) CH claims across relevant CCMDs in the past year	Search and merge unstructured data.
			Ingest data from multiple sources.
			Perform basic analysis with descriptive statistics on metadata from unstructured data.
CCMD	Identify whether CH has occurred within the last five years within AOR.	Count of substantiated CH claims over the last five years within the CCMDs	Ingest data from multiple sources.
			Filter CH investigations by conclusions (i.e., substantiated or not substantiated).
			Perform basic analysis with descriptive statistics on metadata from unstructured data.
CCMD	Identify whether CCMDs have responded to CH incidents over a given period within AOR, and whether those responses have been accepted.	Count and type of CH responses offered. Count and type of CH responses accepted. Full descriptions on how each response was identified as “accepted.”	Ingest data from multiple sources.
			Filter CH investigations by responses (e.g., offered or not offered, accepted or not accepted).
			Perform basic analysis with descriptive statistics on metadata from unstructured data.
IO	Identify whether military operations took	Activity reports (including clandestine	Ingest data from multiple sources.

User	Information Requirement	Data Requirement	Technical Requirements
	place at the time and location where CH was alleged.	operations) from all forces at the specified time and location.	Encrypt data at rest and in transit. Supplement provided metadata with additional classification and dissemination guides as needed.
CP CoE	Identify conditions (e.g., weather, munitions, delivery platform) that may contribute to CH.	List of all operations, each operation tagged as resulting in substantiated instance of CH or not. Data describing operation characteristics including weather, munitions, and delivery platform.	Ingest data from multiple sources. Filter operations by characteristics (e.g., weather, munitions, delivery platform). Perform basic analysis with descriptive statistics on metadata from structured data.

Proposed Transition Action 4: Engage the CHMR community of interest to develop and refine DMP technical requirements. (DART)

Identifying technical requirements that span multiple users and information requirements may help inform selection of an MVP. Selection of an MVP is described in the following section.

1. Consideration: Prioritizing for an MVP

The CHMR-AP describes the DMP as an enterprise-wide, comprehensive database for CH, operational reporting, and data management. Meeting this vision will be a long-term effort; a near-term DMP MVP will need to prioritize users and activities with the ability to scale up. Based on work with the vignettes, the following when prioritizing:

- Prominent Key Users:** Assessing user roles across vignettes indicates the CCMD and IO roles appear most often. As the primary execution arm of DoD operations, CCMDs are poised to initiate CH investigations and implement CHMR recommendations. IOs require access to authoritative data in order to perform investigations. They are the CCMD CDR's designated lead for

understanding specific incidents, providing lessons learned, and making recommendations to the CCMD. Investigations are a powerful tool to drive organizational and cultural changes, highlighting the IO as a prominent key user.

- **Relevant Scenarios:** The vignettes most relevant to CCMDs today should be most highly prioritized. The DoD regularly executes targeting tasks and missions across multiple CCMDs. These missions have resulted in CH, and these mission sets will be components of the Department's CH reporting requirements in the future. Targeting processes are well-defined,¹⁷ repeatable, and supported by systems that generate a robust set of digital artifacts.
- **Prioritized Functionality:** Key users will need to access authoritative data sources, leverage workflow management tools, and capture lessons learned. A DMP MVP may initially prioritize the ability to track incidents, record CCMD actions, and capture lessons learned.
- **Beneficial System Connections:** The OBJ 6 TEM found that certain systems contain large amounts of DMP-relevant data. For example, the Modernized Integrated Database (MIDB) is the primary system supporting targeting. MIDB contains Combat Assessments (i.e., the institutionalized processes within the larger targeting task), Collateral Damage Assessments, Battle Damage Assessments, and Munitions Effectiveness Assessments—all relevant to assessing, investigating, and mitigating CH. MIDB provides access to digital artifacts useful to both CCMDs and IOs and contains information from multiple other repositories. As such, MIDB may prove a high-value addition to the MVP.

Prioritization decisions will inform MVP structure. Figure 4-2 depicts an MVP exemplar that supports the CCMD, IO, and CP CoE users and focuses on performing automated reporting and recording activities. In this MVP, the DMP core begins as an investigation tracker that manages the CH allegation, assessment, and investigation work flow; records actions and outcomes in a data lake; and permits the CP CoE to perform analytics on the stored information in the data lake.

¹⁷ See Joint Publication 3-60 and Chairman of the Joint Chiefs of Staff Instruction 3162.02.

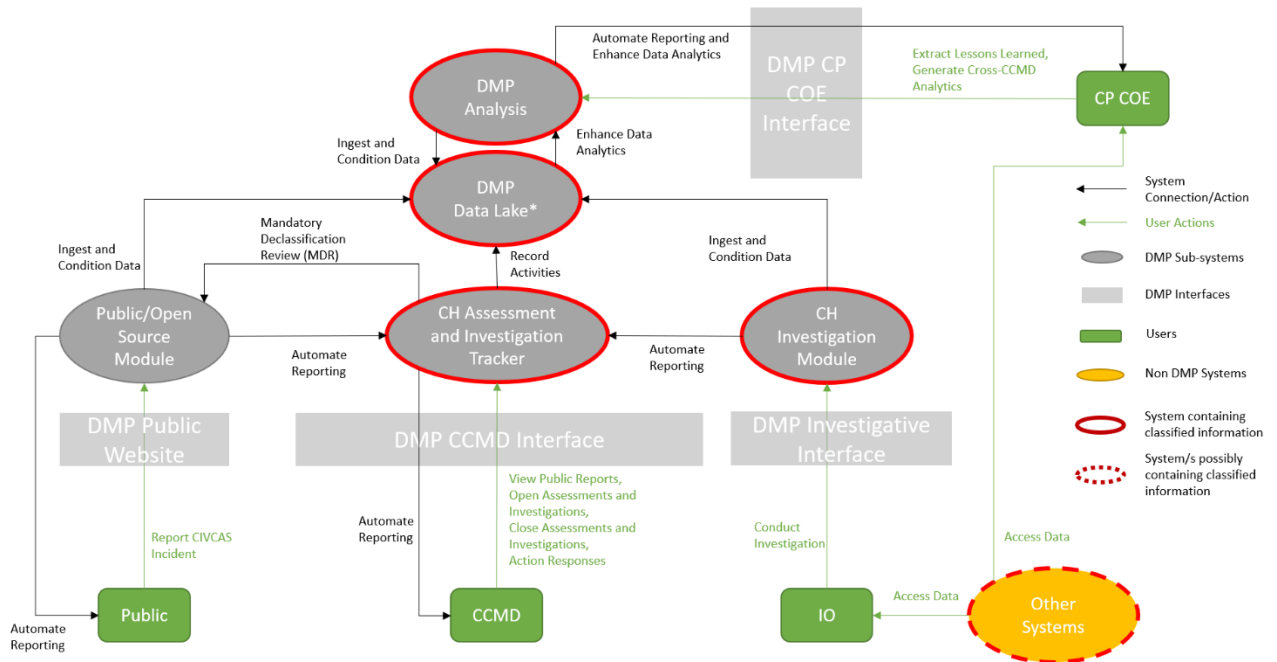


Figure 4-2. Example MVP Prioritizing CCMD, IO, and CP CoE Users, Automated Reporting, and Activity Recording

Given that the MVP shown in Figure 4-2 is focused on automating reporting and recording activities, the MVP does not connect directly to other systems. Instead, the IO and CP CoE user directly access other data systems as needed for their roles. Figure 4-3 depicts a second phase build of the MVP that includes direct connections to other systems. Building an MVP as shown in Figure 4-3 allows business process and data standards to be established before attempting system-to-system connections.

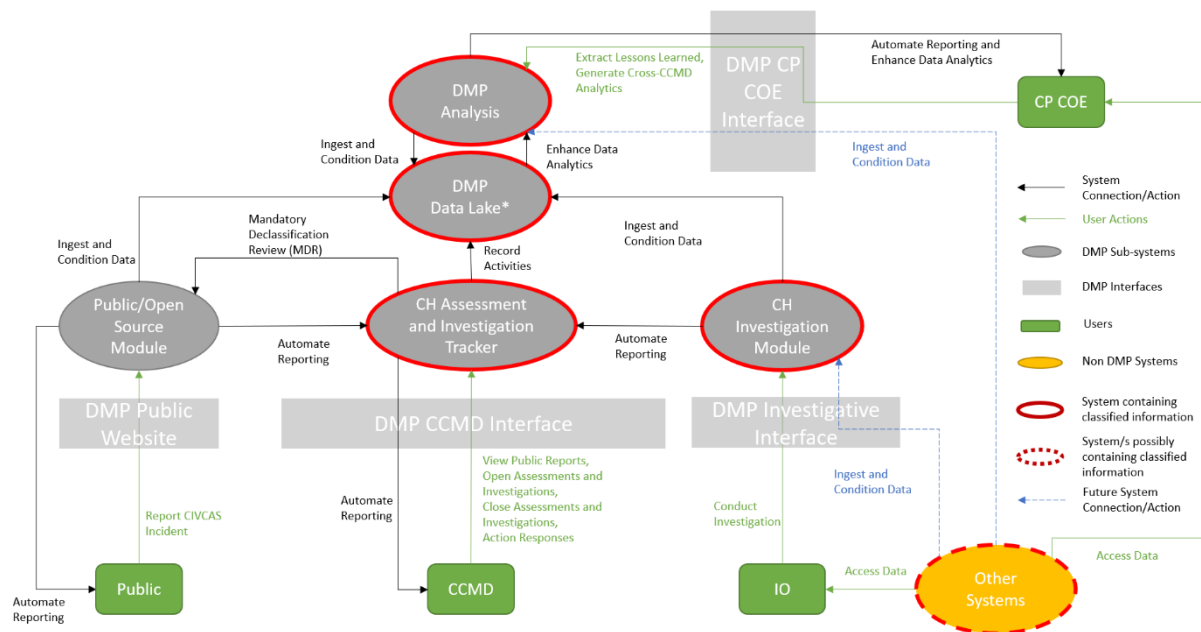


Figure 4-3. Example MVP1 Maturation and Build Out

Proposed Transition Action 5: Leverage information requirements, data requirements, and data sources to prioritize technical requirements for MVP. (DART)

D. Action 6.h

CHMR-AP 6.h: The joint proponent for CHMR, in coordination with DoD CIO, USD(A&S), USD(I&S), and Joint Staff, selects from existing programs, develops, or contracts for a data management platform that meets both technical and information requirements. The joint proponent for CHMR develops the required capability

An analysis of alternatives (AoA) can be leveraged as part of platform selection (Action 6.h). The AoA should consider DMP evaluation criteria, including technical requirements, platform cost, and projected functionality—for example, interaction with open-source reporting, use of data analytics, data retention, maintainer training, security, and potential to scale during armed conflict.

Proposed Transition Action 6: Identify candidate platforms, including existing platforms and a build option, for AoA. (CP CoE & DART)

1. Considerations: Platform Evaluation Criteria

A platform should be selected on the basis of evaluation criteria needed to meet initial and end-state objectives. The DMP will support collecting, aggregating, maintaining, and analyzing CHMR-related information. The DMP may draw on a breadth of data, including operational data, CH claims, CH investigation reports, and metadata from prior analyses. In addition to the standard data life cycle (i.e., data ingest through archival and deletion), the DMP may need to manage multiple applications processing large amounts of data across geographical locations and classification levels.

DMP evaluation criteria should be informed by its system type. Given the information the DMP must provide, it appears more aligned with a business system than a national security system. A business system is operated by, for, or on behalf of the DoD¹⁸ and may focus on a variety of data types (e.g., financial, contracting, logistics, planning and budgeting, installations management, human resources management, training and readiness). In contrast, national security systems are rigidly defined as telecommunications or information systems that involve intelligence activities, cryptologic activities, command and control of military forces, equipment integral to weapons or weapons systems, or administrative or business applications critical to the direct fulfillment of military or intelligence missions.¹⁹ Defining the DMP as a business system would shape evaluation criteria. For example, the DMP should maintain availability but would, as a business system, likely not require a hot-failover site. Tailoring DMP evaluation criteria consistent with its system type facilitates cost-effective infrastructure development.

DMP evaluation criteria should include the following:

- **Technical Requirements:** Technical requirements establish minimum standards for open architecture, data management, hosting and security, and life-cycle support. Comparing performance across candidate platforms may demonstrate that products prioritize different technical areas. Evaluators will need to weigh the benefits of candidate platforms that appear ready to deploy versus those that would require additional configuration to meet technical requirements.
- **User Experience:** If a DMP user cannot navigate the platform effortlessly, workflow will suffer and productivity will fall. Any user interface should be intuitive and easy to navigate, both within and across functions, while still providing users with access to key tools. The platform should prioritize a streamlined user interface.

¹⁸ DoDI 5000.75, “Business Systems Requirements and Acquisition,”

¹⁹ [https://uscode.house.gov/view.xhtml?req=\(title:40%20section:11103%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:40%20section:11103%20edition:prelim))

- **Integration and Interoperability:** The platform should be able to integrate new components (e.g., data sources and analysis tools) into the existing product ecosystem and share information between the product and external applications.
- **Encryption:** The platform should support encryption of data in transport within the platform, encrypting data at rest in the platform, and decrypting encrypted data from outside of the platform.
- **Identity and Access Management (IAM):** IAM is the mechanism for determining the identity of who or what is trying to access a system and controlling access to resources within that system based on the determined identities. The platform may manage multiple systems and should provide convenient IAM support as users cross the boundaries of each system in the platform during standard workflows. Support for RBAC would enable access to the correct personnel while keeping the sensitive data on CH separate from the wider audience (i.e., those without need-to-know). DMP users will span multiple geographic locations. Underlying infrastructure should therefore support global access, and have supporting network infrastructure at user locations. Access mechanisms should be decided and the infrastructure evaluated based on support. For example, if a web page is chosen to present information to users, a DMZ should be in place to support secure access.
- **Regulatory Compliance:** Any platform selected or built should comply with all appropriate security regulations the DoD requires. For example, all cloud-service providers are required to comply with FedRAMP standards. The platform may be subject to other regulatory requirements as well, such as the Federal Information Security Management Act (FISMA) and International Organization for Standardization (ISO) security standards.
- **Data Classification and Migration:** The platform should support access to and data storage of Secret information, while supporting inputs from unclassified data sources. Processes that incorporate higher-level classified networks may also be considered. The platform should properly label and restrict access to or dissemination of data based on the data's classification.
- **Auditability:** Platform managers should be able to access a complete view of the amount, type, location, and classification of data residing in the platform. They should also be able to obtain a complete view of the users accessing data, including when and where user's access data and logs of previous access. The platform should allow view of investigation workflow, including initial CH claims and final reports, for each investigation.
- **Multiple Database Structures and Inter-database Communication:** The platform will likely need to manage both structured and unstructured data.

Unstructured data may include free text from previously written investigation reports and assessments, free text from CH claims, and free text from open source news channels. Structured data may include times, weapons systems, names, and locations. The platform should support sharing and aggregating this disparate data, spanning different databases as needed. The platform should support data standardization where feasible (e.g., by prescribing the format of data sent across components within the platform).

- **Performance:** The platform will be accessed across geographic locations and possibly from remote positions without high bandwidth. Supporting DMP data access across all geographies within minutes of its upload requires low latency.
- **Cost:** The CHMR-AP offers the option to adopt an existing solution or build a platform. In either case, procuring, developing, sustaining, and securing the DMP have associated costs. Evaluators should more accurately define the actual cost of each option by performing a comprehensive cost comparison that accounts for different pricing strategies and possible discounting.

Proposed Transition Action 7: Perform an AoA to select a platform that meets DMP evaluation criteria—focusing on technical requirements at the MVP stage—and can scale to meet DMP needs once the platform reaches FOC. (CP CoE & DART)

E. Action 6.i

CHMR-AP 6.i: *The joint proponent for CHMR, in coordination with DoD CIO and USD(A&S), refines cost estimates associated with the data management platform over time and provides such estimates to CHMR SC for incorporation into budget requests.*

Any refinements to procurement, development, and sustainment plans should be considered in cost updates. Additions to required DMP data sources and changes in DMP functionality may also drive cost estimates. For example, DMP costs are likely to increase as interoperability requirements grow more complex.

Proposed Transition Action 8: Refine DMP cost estimates to include considerations related to platform selection, MVP development, and sustainment as the DMP progresses toward FOC. (CP CoE)

F. Action 6.j

CHMR-AP 6.j: *Joint Staff and combatant commands establish standardized processes for reporting civilian harm. Specifically:*

- i. Update and disseminate the Chairman's Critical Information Requirements Reporting Matrix to all military departments, combatant commands, and interagency partners; and*
- ii. Establish combatant command reporting criteria.*

A 2019 DoD Report on Civilian Casualty Policy²⁰ found a lack of uniform processes and standards across CCMDs for investigating, acknowledging, and responding to CH. These non-standard processes work against consolidated CH reporting and hinder efforts to improve CHMR tactics, techniques, and procedures. Standardizing processes moves the DoD closer to these goals.

Although this action is assigned to CCMDs and the Joint Staff, the CP CoE may benefit from partnering to ensure the DMP supports any resulting processes. Successfully establishing standardized processes that integrate well with the DMP would require close coordination between CCMDs (as mission operators), the Joint Staff (as the process-generating entity), and the CP CoE (as DMP manager).

Proposed Transition Action 9: Coordinate with Joint Staff and CCMDs to ensure the DMP supports any standardized processes developed. (CP CoE)

²⁰ <https://media.defense.gov/2019/Feb/08/2002088175/-1/-1/1/DOD-REPORT-ON-CIVILIAN-CASUALTY-POLICY.PDF>

5. Phase 2 (FY24) and Phase 3 (FY25) Considerations

A. Phase 2 (FY24) Considerations

CHMR-AP 6.k: *The joint proponent for CHMR submits a FY25 Issue Paper for enduring CHMR requirements in FY25 and beyond, based upon the findings of the CHMR manpower study and any other resourcing requirements that are identified. If needed, the joint proponent for CHMR, in coordination with USD(C), DoD GC, and ASD(LA), also develops any necessary legislative proposals for consideration within the DoD Legislative Program.*

CHMR-AP 6.l: *The joint proponent for CHMR develops and distributes Standard Operating Procedures (SOP) for the data management system.*

CHMR-AP 6.m: *The joint proponent for CHMR coordinates with the platform developer and the CP CoE to develop and provide training across the joint force for relevant data managers and units.*

The standard operating procedures (SOPs) prescribed in Action 6.l should include guidance for DMP users performing data management roles and responsibilities (e.g., provisioning, development, sustainment, and security). These SOPs will need to prescribe activities in a manner supportive of standardized outputs. These SOPs should also shape the training specified in Action 6.m.

Proposed Transition Action 10: Develop and distribute DMP SOPs. Coordinate with the DMP developer to create and provide training to data managers and units as appropriate.

B. Phase 3 (FY25) Considerations

CHMR-AP 6.n: *Combatant commands and other relevant DoD and OSD components employ the data management tool as the authoritative platform for the collection of CHMR reporting and data management.*

Action 6.n directs employing the DMP as the authoritative reporting tool. To support this, users (i.e., CCMDs, CHMROs, CHACs, IOs) should employ the DMP in a consistent manner. DMP output becomes harder to standardize if two CCMDs leverage the platform differently.

Proposed Transition Action 11: Coordinate with DMP users to support standard utilization of the DMP by those with the same roles. Brief the CHMR Steering Committee on CCMD DMP adoption.

6. Summary of Transition Actions

Table 6-1 summarizes recommended actions to complete Phase 1, Phase 2, and Phase 3, in support of DMP development, sustainment, and use. These actions, organized by phase and entity, are designed to help guide the CP CoE and DART through the strategic roadmap and toward DMP FOC.

Table 6-1. Summary of Proposed Transition Actions

CHMR-AP Phase	CHMR-AP Action	Proposed Lead	Proposed Transition Actions
Phase 1 (FY23)	6.f	CP CoE	Adopt a data call to identify data system points of contact.
	6.f	CP CoE	Manage refinements to DMP information requirements and data sources as CHMR roles and processes mature.
	6.g	DART	Align information requirements (Appendix D) to data sources (Appendix E) via data requirements.
	6.g	DART	Engage the CHMR community of interest to develop and refine DMP technical requirements.
	6.g	DART	Leverage information requirements, data requirements, and data sources to prioritize technical requirements for MVP.
	6.h	CP CoE & DART	Identify candidate platforms, including existing platforms and a build option, for AoA.
	6.h	CP CoE & DART	Perform an AoA to select a platform that meets DMP evaluation criteria—focusing on technical requirements at the MVP stage—and can scale to meet DMP needs once the platform reaches FOC.
	6.i	CP CoE	Refine DMP cost estimates to include considerations related to platform selection, MVP development, and sustainment as the DMP progresses toward FOC.
	6.j	CP CoE	Coordinate with Joint Staff and CCMDs to ensure the DMP supports any standardized processes developed.

CHMR-AP Phase	CHMR-AP Action	Proposed Lead	Proposed Transition Actions
Phase 2 (FY24)	6.l, 6.n	CP CoE	Develop and distribute DMP SOPs. Coordinate with the DMP developer to create and provide training to data managers and units as appropriate.
Phase 3 (FY25)	6.n	CP CoE	Coordinate with DMP users to support standard utilization of the DMP by those with the same roles. Brief the CHMR Steering Committee on CCMD DMP adoption.

The strategic roadmap in Figure 6-1 provides a phased array of actions across multiple operational imperatives. The roadmap supports immediate and long-term tasks tied to end state objectives, thereby aligning near-term actions to long-term outcomes consistent with the CHMR-AP.

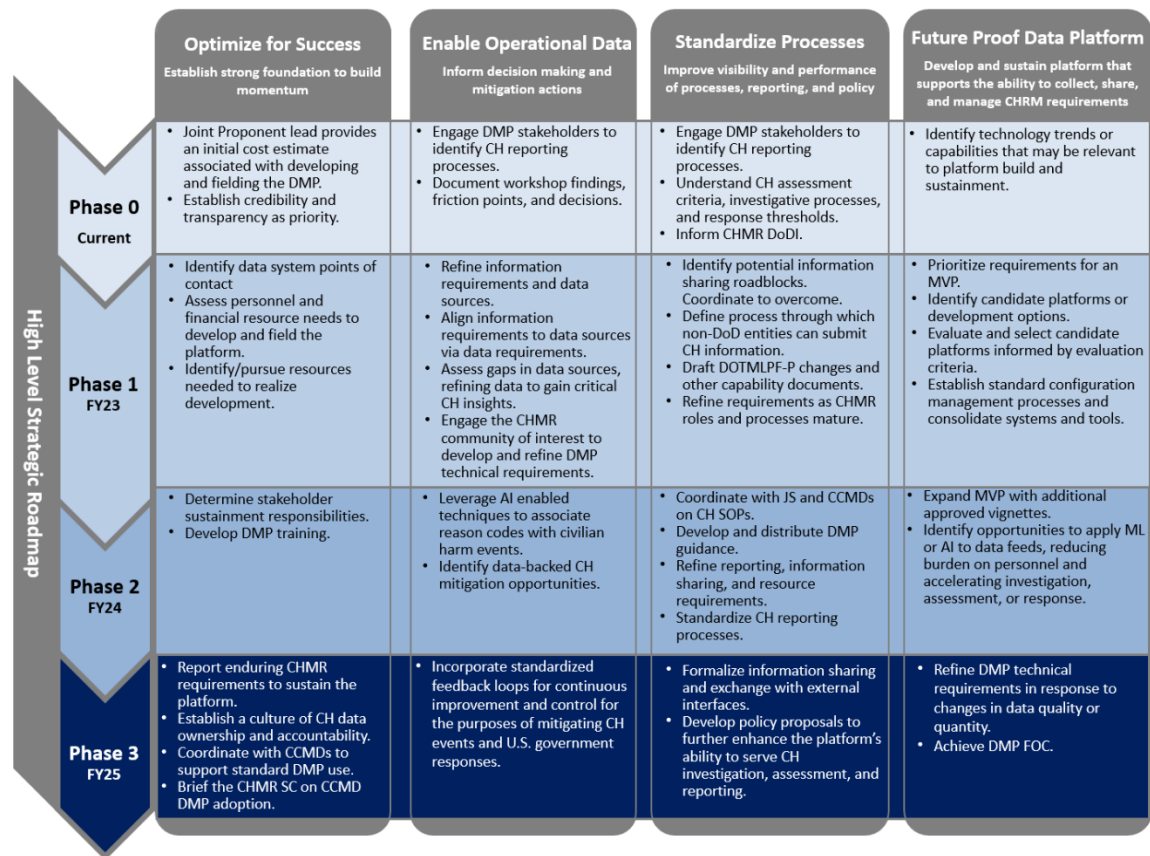


Figure 6-1. DMP Strategic Roadmap

Appendix A. CHMR Policy Background

A. What Federal-level Policies Govern CH Reporting in the DoD?²¹

Research shows National Defense Authorization Acts (NDAAAs) driving Federal-level policies concerning CH, reporting, and restitution. Table A-1 accounts for Federal-level policies dealing directly with civilian casualties or CH resulting from U.S. military operations.

Table A-1. Federal-level Policies on CH Due to U.S. Military Operations

Policy Type	Document Name	Publication Date
Executive Order (E.O.)	E.O. 13732, United States Policy on Pre- and Post-Strike Measures to Address Civilian Casualties in U.S. Operations Involving the Use of Force	1-Jul-2016
NDAA	FY2019 NDAA, Sec. 936. Responsibility for Policy on Civilian Casualty Matters.	13-Aug-2018
DoD Report	Report on Civilian Casualty Policy (Response to FY2019 NDAA, Sec. 936)	1-Feb-2019
NDAA	FY2022 NDAA, Sec. 1331. Extension and Modification of Authority for Certain Payments to Redress Injury and Loss.	27-Dec-2021
NDAA	FY2023 NDAA, Sec. 1082. Department of Defense Civilian Protection Center of Excellence.	23-Dec-2022

The FY2019 NDAA required a report on civilian casualty policy within 90 days of the legislation's passage. The subsequent DoD Report on Civilian Casualty Policy, published in February 2019, references relevant Chairman of the Joint Chiefs of Staff (CJCS), Military Service, and CCMD policies. The DoD Report on Civilian Casualty Policy also discusses a draft DoD policy. According to the report, this draft DoD policy will give guidance on recording kinetic U.S. military strikes, developing a mechanism for the public

²¹ Research as of February 2, 2023.

to report CIVCAS of U.S. military operations, reviewing and investigating such reports, and addressing harms determined to have occurred, whether in acknowledging responsibility or issuing *ex gratia* payments.

Section 1213 of the FY 2020 NDAA appropriates no more than \$3 million per calendar year for the Office of the Secretary of Defense under the Operation and Maintenance, Defense-wide account. These funds are for *ex gratia* payments for damage, personal injury, or death as a result of the use of force by the U.S. military.²² This payment is not considered an admission or acknowledgement of any legal obligation to provide compensation. This Section stipulates that local military commanders must receive legal advice prior to making payments, must keep a written record of payments, and must submit this record to “the appropriate office in the Department of Defense as determined by the Secretary of Defense.” The Secretary must then report on *ex gratia* payment requests to Congressional defense committees every 90 days, regardless of whether a payment was made. This section was later amended by Sec. 1331 of the FY2022 NDAA to require the Secretary of Defense to receive, evaluate, and respond to allegations of CH resulting from U.S. military operations.²³

Section 1082 of the FY2023 NDAA establishes the DoD CP CoE, which is referred to by name in the CHMR-AP.²⁴ The CP CoE serves as the focal point for matters related to civilian casualties and other forms of CH resulting from military operations involving the United States Armed Forces.²⁵ The CP CoE is also responsible for institutionalizing and advancing knowledge, practices, and tools for preventing, mitigating, and responding to CH. The Secretary of Defense must report annually on CP CoE activities to Congressional defense committees.

In addition, E.O. 13732 (2016) directs U.S. departments and agencies to conduct assessments aimed at reducing civilian casualties and to maintain channels for engagement with foreign partners, the international Committee of the Red Cross, and other non-governmental organizations. This E.O. also stipulates that the Director of National Intelligence (DNI) shall release an annual report on “the number of strikes undertaken by the U.S. Government against terrorist targets outside areas of active hostilities [that year], and assessments of combatant and non-combatant deaths resulting from those strikes.”²⁶

²² <https://www.congress.gov/bill/116th-congress/senate-bill/1790/text>

²³ <https://www.congress.gov/bill/117th-congress/senate-bill/1605/text>

²⁴ <https://media.defense.gov/2022/Aug/25/2003064740/-1/-1/1/CIVILIAN-HARM-MITIGATION-AND-RESPONSE-ACTION-PLAN.PDF>

²⁵ <https://www.congress.gov/bill/117th-congress/house-bill/7776/text?s=6&r=2&q=%7B%22search%22%3A%5B%22fy+2023+ndaa+final%22%5D%7D>

²⁶ <https://www.govinfo.gov/content/pkg/DCPD-201600443/html/DCPD-201600443.htm>

B. What Army Policies Offer Guidance on CH Mitigation and Reporting?

Five Army publications, two cross-listed as Marine Corps Field Manuals, offer insights into Service-level policies on CH and civilian casualties. These are listed in Table A-2. Deeper analysis of each is warranted, but selected excerpts are below.

Table A-2. Service-level Policies on CH

Document Name	Publication Date
ATP 3-07.6: Protection of Civilians	18-Jul-2012
FM 3-24/MCWP 3-33.5: Insurgencies and Countering Insurgencies	1-May-2014
ADP 3-37: Protection	11-Dec-2018
AR 638-8: Army Casualty Program	7-Jun-2019
FM 6-27/MCTP 11-10C: The Commander's Handbook on the Law of Land Warfare	1-Aug-2019

ATP 3-07.6: Protection of Civilians:

ATP 3-07.6 contains five chapters:

Chapter 1 provides an overview of the protection of civilians, discusses its legal underpinnings, and addresses considerations including civilian risks. It discusses civilian protection during military operations and introduces the protection of civilians framework used in the document, which includes three components: understanding civilian risks, conducting operations to protect civilians, and shaping a protective environment.

Chapter 2 addresses situational understanding of civilian risks. It discusses civilian protection in the context of an operational environment, intelligence activities, information sharing, and assessments.

Chapter 3 discusses the relationship of the operations process and the warfighting functions to the protection of civilians. It also discusses the conduct of operations that support the protection of civilians.

Chapter 4 describes the relevance of governance, rule of law, conflict-related sexual violence, protection of children, and other issues for achieving enduring protection of civilians. It also discusses the importance of a comprehensive approach that engages the population, host nation leaders and organizations, and other actors.

Chapter 5 discusses the mitigation of civilian casualties, including preventive measures and methods to address civilian casualties that occur.

FM 3-24/MCWP 3-33.5: Insurgencies and Countering Insurgencies:

13-22. The civilian population and individual civilians not taking a direct part in hostilities are protected from intentional attack. Where civilians are present on the battlefield or in proximity to legitimate military objectives, or they are being used to shield legitimate targets from an attack that otherwise would be lawful, they are at risk of injury incidental to the lawful conduct of military operations. A law of war violation occurs when—

- The civilian population is attacked intentionally.
- Civilian casualties incidental to an otherwise lawful attack become excessive in relation to the concrete and direct military advantage to be gained and are attributed to the wanton conduct of an attacking force, for which the defending force or individual civilians or groups of civilians (such as voluntary human shields) bear no responsibility.
- A defender or attacker employs civilians as voluntary or involuntary human shields. Each of these acts constitutes a violation of the principle of discrimination. 13-23. The law of war does not expressly prohibit civilians from taking a direct part in hostilities. If they do, however, they may be targeted for so long as they take a direct part. Civilians do not enjoy the combatant's privilege—that is, they do not have combatant immunity—and if captured, they may be prosecuted for their belligerent acts under the domestic law of the captor.

ADP 3-37: Protection:

5-39. Army units should account for the protection of civilians from other hazards, in addition to their own direct and indirect fires. Particularly in counterinsurgency and when executing stability task situations, population support may be the center of gravity; and it is unlikely that support can be achieved if the population is not protected. Army units may be expected to take measures that protect civilians from enemy or adversary actions. AT measures should also account for the protection of civilians, as they are likely to become incidental casualties by deliberate attacks against soft and populated targets.

5-40. Civilian casualty mitigation is similar to fratricide avoidance, as both are intended to avoid casualties upon an unintended target. The mitigation of civilian casualties is more challenging because there tends to be a high density of civilians throughout the area, in unexpected locations, and outside the command chain. In many cases, civilians are virtually indistinguishable from the enemy or adversary. In the same way that Army units continually consider the possibility of fratricide and take measures to mitigate its risk, they should adopt a similar mind-set regarding the avoidance of civilian casualties.

AR 638-8: Army Casualty Program:

Chapter 4: Casualty Notification, Section I: Notification Tradition/Notification Requirements for Deceased, 4-1. Casualty notification for deceased.

It is DOD policy to make personal notification to NOK for deceased, DUSTWUN, and EAWUN cases. Notification or condolences are required for all reportable casualties in accordance with DODI 1300.18. A uniformed Service representative (except for notification of contractors) will promptly notify the NOK in an appropriate and dignified manner. They will also make personal notification to the PNOK of separated and retired personnel when these personnel become a casualty overseas and the PNOK is located in the United States or vice versa, if requested. When a Soldier or DOD and/or DA Civilian is reported as deceased, DUSTWUN, or EAWUN, the following actions apply:...

h. The CMAOD will apprise the Assistant G-1 for Civilian Personnel (DAPE-CPZ) POC for DA Civilian casualties.

i. For DOD Civilian casualties belonging to the DOD Components listed in DODI 1300.18, paragraph E6.1.2, CMAOD will notify the respective designated military Service and provide any necessary casualty assistance. If the respective agency requests Army assistance in making notification, CMAOD will coordinate with the appropriate CAC to arrange for a notification team.

FM 6-27/MCTP 11-10C: The Commander's Handbook on the Law of Land Warfare

Feasible Precautions in Planning and Conducting Attacks to Reduce the Risk of Incidental Harm

In planning and conducting attacks, combatants should take feasible precautions to reduce the risk of incidental harm (see DOD Law of War Manual, 5.11; consider AP I art. 57). What precautions are feasible depends greatly on the context, including operational considerations. Examples of precautions in conducting attacks that may be feasible sometime include: warning before attack, adjusting the timing of the attack, selecting certain weapons to use in the attack, assessing the risk to civilians, identifying zones in which military objectives are more likely to be present or civilians are more likely to be absent, and canceling or suspending an attack based on new information that raises concerns of expected civilian casualties (see DOD Law of War Manual, 5.11).

5-3. Commanders, at all levels, have a great responsibility to exercise the leadership necessary to reduce the risk of harm to civilians and civilian objects. Accordingly, they should, for example:

- Make the necessary judgments and decisions required by the principle of proportionality to ensure that harm to civilians and civilian objects is not excessive compared to the expected military advantage.

- Determine the feasible precautions to take for the protection of civilians in planning and conducting an attack, including canceling or suspending an attack based on new information raising concerns of expected civilian casualties or determining whether it is feasible to provide warnings or to use different types of weapon systems to reduce the risk of civilian casualties) (see DOD Law of War Manual, 5.11).
- Administer civilian internment camps in accordance with the GC.
- Arrange for passage of humanitarian relief.

Appendix B. OBJ 6 Working Group Members

Table B-1 lists all individuals who participated in the OBJ 6 Working Group either in person at the OBJ 6 Technical Exchange Meeting or online in team meetings.

Table B-1. OBJ 6 Working Group Participants

Command	Name	NIPR
Army, HQDA G/3-5-7	SES Adam Nucci	adam.j.nucci.civ@army.mil
Army, HQDA OSA-OBT (DART)	SES Daniel Jensen	daniel.c.jensen.civ@army.mil
Army, HQDA G/3-5-7	COL Steven Gandia	steven.gandia.mil@army.mil
Army, HQDA G/3-5-7	MAJ Cory Scharbo	cory.r.scharbo.mil@army.mil
Army (CP CoE)	COL “Nady” Pierre	joseph.n.pierre.mil@army.mil
Army PA	Madison Bonzo	madison.t.bonzo.civ@army.mil
Army, CAC	Mark Murphy	mark.j.murphy2.civ@army.mil
Army, Manpower Analysis Agency	Mike Yocum	james.m.yocum2.civ@army.mil
Army	COL Assia-Leila Green	assia-leila.green.fm@army.mil
Army	Kurt Takushi	kurt.a.takushi.civ@army.mil
Army	Randy Lane	randall.c.lane.civ@army.mil
AFRICOM	COL Landon Quan	landon.e.quan.mil@mail.mil
Air Force	Francis Scolaro	francis.scolaro.3@us.af.mil
Air Force	Ms. DonnaMarie Stitham	donnamarie.stitham@us.af.mil
Air Force	MSgt Tiffany Cannon	tiffany.cannon@spaceforce.mil
Air Force	Thomas Moon	thomas.moon.1@us.af.mil
CDAO	Jenny Sue Ross	jennifer.s.ross13.civ@mail.mil
CDAO	MAJ Phillip Cho	philip.y.cho.mil@mail.mil
CDAO	Regina McCoy	regina.mccoy.ctr@mail.mil
DIA	Kathleen Todd	Kathleen.Todd2@dodiis.mil
DIA	Michael Jackson	Michael.Jackson@dodiis.mil
DSCA	Melissa Carlson	melissa.a.carlson16.civ@mail.mil
IDA	Laura Odell	lodell@ida.org
IDA	Cameron DiLorenzo	cdiloren@ida.org
IDA	Claire Haas	chaas@ida.org
IDA	Todd Sabala	tsabala@ida.org
IDA	Miranda Seitz-McLeese	mseitzmc@ida.org
IDA	Cliff Bridges	cbridges@ida.org
JS J2	Amanda Corsetti	amanda.l.corsetti.civ@mail.mil
JS J2	CAPT Mar Chaudhry	mariyah.q.chaudhry.mil@mail.mil

Command	Name	NIPR
JS J2	Christina Maiava Schaff,	christina.m.schaff.civ@mail.mil
JS J2	JS J2T	js.pentagon.j2.list.j2t-doctrine--policy-div@mail.mil
JS J2	Tony Barker	tony.l.barker.civ@mail.mil
JS J2	Venessa Lantrip	venessa.a.lantrip2.mil@mail.mil
JS J2F	Tony Barker	tony.l.barker.civ@mail.mil
JS J3	LT COL Kenneth Brakora	kenneth.m.brakora.mil@mail.mil
JS J5	LT COL Gregory DeGruchy	gregory.a.degruchy.mil@mail.mil
JS J5	LT COL Kelly Padden	kelly.a.padden.mil@mail.mil
JS J8	CDR Peter Gaal	peter.a.gaal.mil@mail.mil
JTCG/ME	Christopher Maxie	christopher.m.maxie2.civ@army.mil
Navy	Jim Custer	james.custer@navy.mil
Navy	Mr. Dave Pettitt	david.g.pettitt.ctr@us.navy.mil
Navy	Mr. Rajat Roy	rajat.s.roy.civ@us.navy.mil
Navy	Robert Lewis	robert.lewis9.ctr@navy.mil
NGA	COL Daniel j. Benick	daniel.j.benick.mil@army.mil
NGA	Daniel Benick	daniel.j.benick.mil@army.mil
Oak Ridge National Labs	Marie Urban	urbanml@ornl.gov
OSD (R&E)	Chris Deluca	ralph.c.deluca.civ@mail.mil
OSD(A&S)	CAPT Robert “Mac” McFarlin	robert.w.mcfarlin.mil@mail.mil
OSD(A&S)	Karin Britt	karin.m.britt.civ@mail.mil
OSD(I&S)	Andrew Loftesnes	andrew.f.loftesnes.ctr@mail.mil
OSD(I&S)	Dan Bernabei (dB)	daniel.a.bernabei.civ@mail.mil
OSD(I&S)	Hugh Curry	harmon.h.curry.civ@mail.mil
OSD(I&S)	Mic Bryant	michael.p.bryant2.ctr@mail.mil
OSD(I&S)	Thomas Tucker	thomas.w.tucker18.ctr@mail.mil
OSD(P)	Elena Crespo	elena.i.crespo.civ@mail.mil
OSD(P)/SOLIC	Dan Stigall	dan.e.stigall.civ@mail.mil
OSD(P)/SPC	Cara Negrette	cara.g.negrette.civ@mail.mil
OSD(PA)	Cesar Santiago-Santini	cesar.h.santiagosantini.mil@mail.mil
OSD(PA)	Kerry Humphrey	kerry.s.humphrey.civ@mail.mil
USAF A2	Thomas Moon	thomas.moon.1@us.af.mil
USCENTCOM	COL Erwin Larios	erwin.a.larios.mil@mail.mil
USCYBERCOM	COL Kyle Baldassari	kmbalda@USCYBERCOM.mil
USCYBERCOM	Jack Schweitzer	jrschw3@USCYBERCOM.mil
USCYBERCOM	LT COL Jacob Portaro	jdporta@USCYBERCOM.mil
USD(I&S)	Daniel Bernanei	daniel.a.bernabei.civ@mail.mil

Command	Name	NIPR
USD(I&S)	Harmon Curry	harmon.h.curry.civ@mail.mil
USEUCOM	COL Jeffrey Crivellaro	jeffrey.c.crivellaro.mil@mail.mil
USEUCOM	MAJ Jeremy Crossman	Jeremy.m.crossman.mil@mail.mil
USINDOPACOM	Jenny McAvoy	jennifer.mcavoy.ctr@pacom.mil
USINDOPACOM	Michael McGregor	michael.v.mcgregor2@pacom.mil
USINDOPACOM	Patrick Gray	patrick.j.gray.civ@us.navy.mil
USNORTHCOM	COL Michael Jones	michael.c.jones.mil@mail.mil
USSOCOM	John Cromer	john.cromer@socom.mil
USSTRATCOM	Mr. Elliot “Sniper” Fair III	elliott.t.fair.civ@mail.mil
USSTRATCOM	Mr. Josh Hoenshell	joshua.k.hoenshell.civ@mail.mil

Appendix C. Vignettes

The IDA team developed five vignettes to identify key users and draw out information requirements (see Figure C-1 for an overview). The subsequent paragraphs introduce each vignette, and bracketed abbreviations introduce key users.

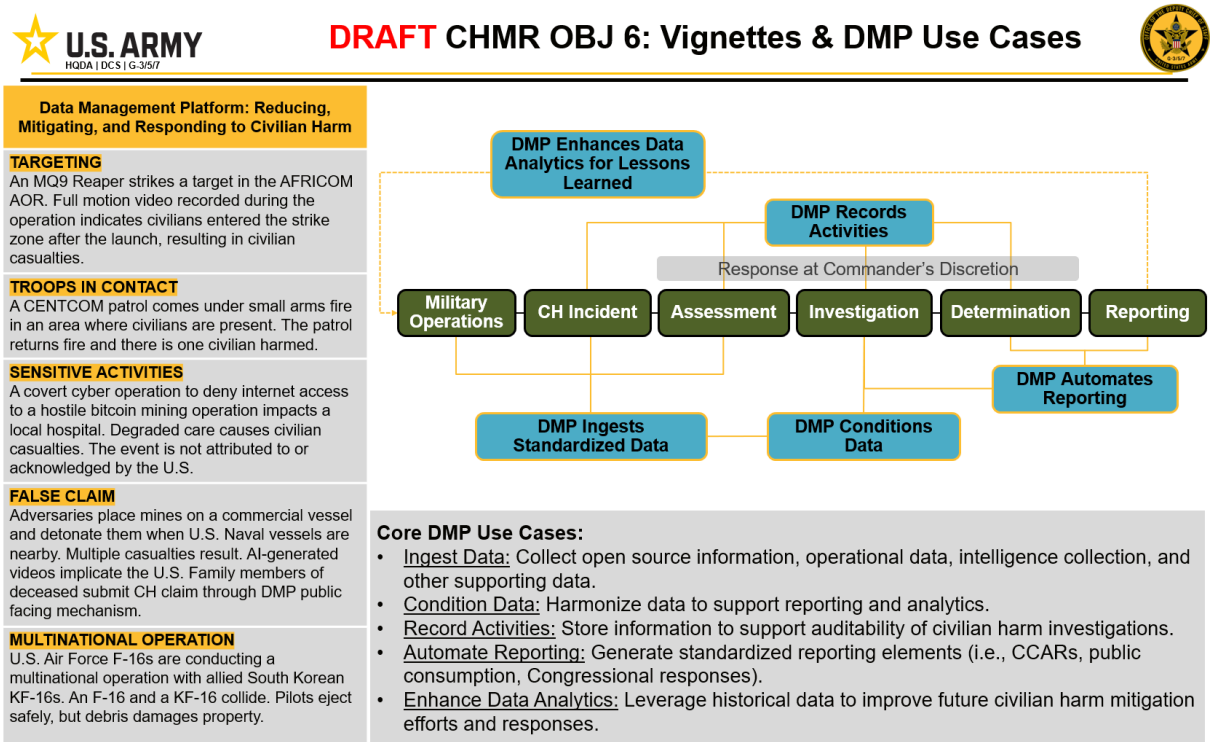


Figure C-1. Vignettes and DMP Use Cases

Targeting Vignette (see Figure C-2 for an overview): AFRICOM identifies a target of interest. Intelligence collection informs target development and validation. The target is struck by an MQ9 Reaper in a pre-determined engagement area. Nearby civilians unexpectedly drive into the target area after missile launch but before impact. This results in CIVCAS. The operators complete a combat assessment, and the strike is captured on full motion video, as are visuals of civilians fleeing the strike site. The CCDR refers the incident to the CHAC, which conducts a CH assessment [CCMD]. Public news outlets report civilian casualties, and social media postings parallel this information. The findings lead to an investigation [IO]. The DMP records the CIVCAS allegation [CCMD], CCAR progress [IO], and the ultimate CIVCAS determination. The allegation is found to be credible [IO]. The Commander recommends a response, which AFRICOM actions [CCMD]. The DMP records this response and outputs standardized reporting [CP CoE].

The DMP facilitates lessons learned, which can be leveraged to inform and enhance future military operations [CP CoE].

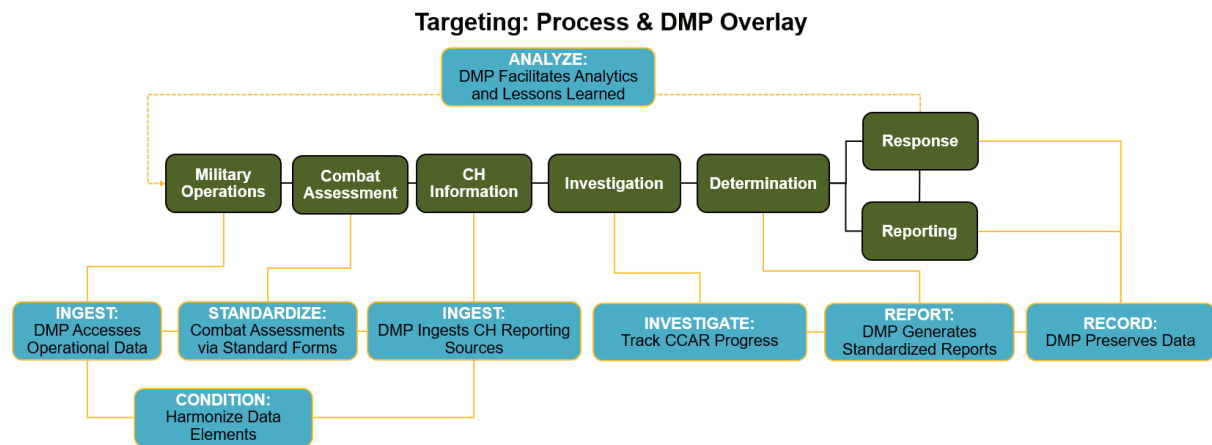


Figure C-2. Targeting Process & DMP Overlay

Troops in Contact Vignette (see Figure C-3 for an overview): A U.S. Army patrol is in the CENTCOM AOR during the conduct of hostilities. When returning from a Key Leader Engagement, the patrol is attacked with direct fire weapons. The patrol returns fire, and the adversary retreats. One civilian, present in the area of operations, is injured. When back from patrol, the Unit Commander—following appropriate chain of command—completes a standardized combat assessment and submits it through appropriate channels [CCMD]. The DMP records this assessment. The DMP performs text analytics and flags the report to the CHAC as a potential CH incident due to the mention of one CIVCAS [CCMD]. An investigation takes place [IO]. The investigating officer records progress and results in the DMP [IO]. The Commander decides on an appropriate response, which is recorded in the DMP to enable automated reporting [CCMD].

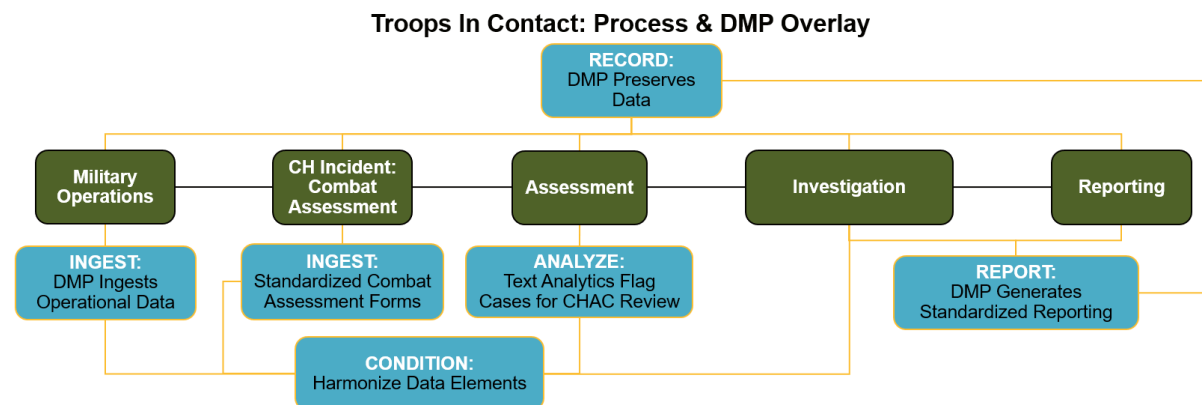


Figure C-3. Troops In Contact Process & DMP Overlay

False Claim Vignette (see Figure C-4 for an overview): Royal Cambodian Navy (RCN) Vessels, U.S. Navy (USN) vessels, and a commercial cargo ship are present in the

Taiwan Strait. Hostile actors place a charge on the cargo ship and detonates it when a USN vessel passes. All inventory and crew are lost. Subsequent reporting and social media postings circulate video showing USN vessels kinetically engaging the cargo ship. Soon after, family members of those aboard the cargo ship submit CH claims through the DMP public access site [P]. The U.S. government initiates an investigation, using the DMP to record the allegation, investigation proceedings, and data generated by the investigative process [CCMD, IO]. The CENTCOM investigating officer (IO) accesses the DMP searching for operational data (i.e., ISR, munitions data) that may indicate the USN vessel engaged kinetically [CCMD, IO]. The IO finds no indication of kinetic activity. A digital forensics investigation indicates videos circulating online appear to be AI generated. The DMP stores these findings, generating both a secret-level and unclassified report reflecting the lack of evidence that the U.S. was involved [CCMD].

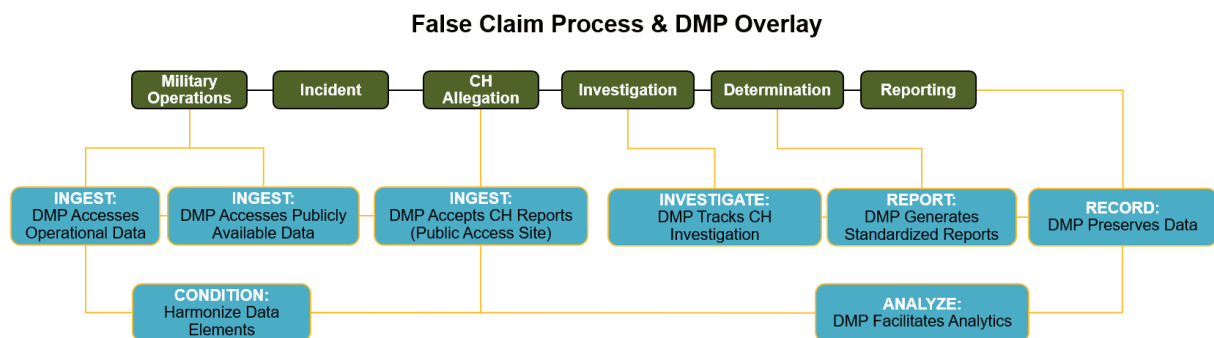


Figure C-4. False Claim Process & DMP Overlay

Multinational Operation Vignette (see Figure C-5 for an overview): U.S. Air Force (USAF) aircraft are conducting a multinational operation with allied South Korean forces in the INDOPACOM region during the conduct of hostilities. A USAF F-16 and a KF-16 collide over South Korean territory. The USAF F-16 crashes in an agricultural area near Osan Air Base. Both pilots eject safely and file an incident report. Local news outlets report that debris damaged a Korean farmer's crops and farming equipment. A Korean civilian submits a CH allegation through official channels (i.e., a public access site hosted by the DMP) [P]. An investigation is conducted, and the DMP records its progress [IO]. The investigating officer (IO) draws on black box data, radio recordings, and radar information to validate that the incident was an accident in the course of operations [IO]. These data objects offer critical data elements—such as date, time, and geolocation—to substantiate the Korean farmer's claims. The IO also references data from Korean systems to corroborate operational facts [IO, Others]. The IO determines the allegation is credible, records this finding in the DMP, and recommends a payment to the farmer [IO]. The Commander actions this response and records it in the DMP [CCMD]. The DMP automatically generates an unclassified report walking through incident occurrence, investigation, and response [CP CoE]. INDOPACOM Civil Affairs shares this report with

the U.S. Embassy in Seoul [CA]. Embassy staff posts this report on the Embassy website to acknowledge the incident.

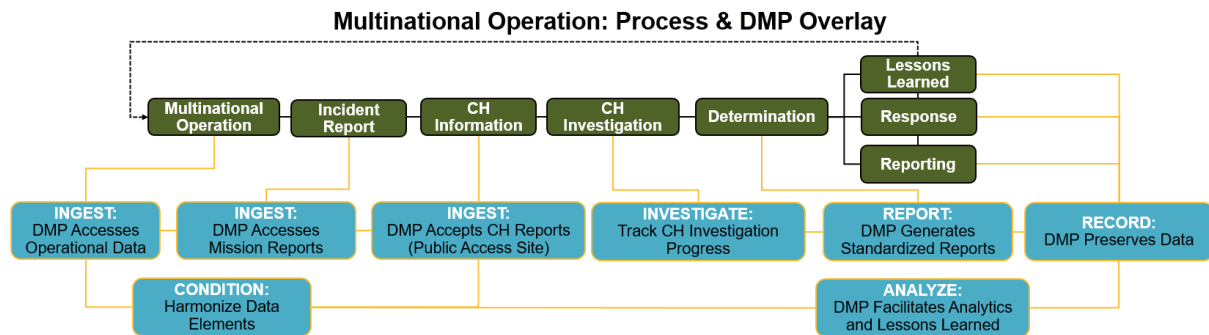


Figure C-5. Sensitive Activities Process & DMP Overlay

Sensitive Activities Vignette (see Figure C-6 for an overview): The U.S. is engaged in hostilities against a terrorist group in the U.S. European Command (EUCOM) AOR. U.S. intelligence indicates the group mines bitcoin to fund its weapons procurement and other activities against U.S. interests. The President directs USCYBERCOM to enact a covert, TS/SCI-level cyber operation that takes the local Internet service provider offline and denies Internet connectivity to the bitcoin mining facility. USCYBERCOM clears this operation through EUCOM prior to acting. Unanticipated operational effects cause a local hospital to lose access to electronic medical records and internet-enabled medical equipment. Dozens of civilians cannot receive proper care and degrade in medical condition. Some die as a result. Consistent with the classification of this operation, the U.S. government does not publicly acknowledge the operation. USCYBERCOM systems record engagement authority, operational data, and operational outcomes [CCMD]. The DMP does not ingest any of this data. USCYBERCOM investigative entities access this data in USCYBERCOM systems during the course of an after-action review, following data structure and analytical standards set by the DMP [CCMD, IO]. The USCYBERCOM CHAC, coordinating as appropriate with the EUCOM CHMRO, generates a standardized lessons-learned document that informs training and future operations [CCMD]. Once declassified, this standardization facilitates ingesting data into the DMP.

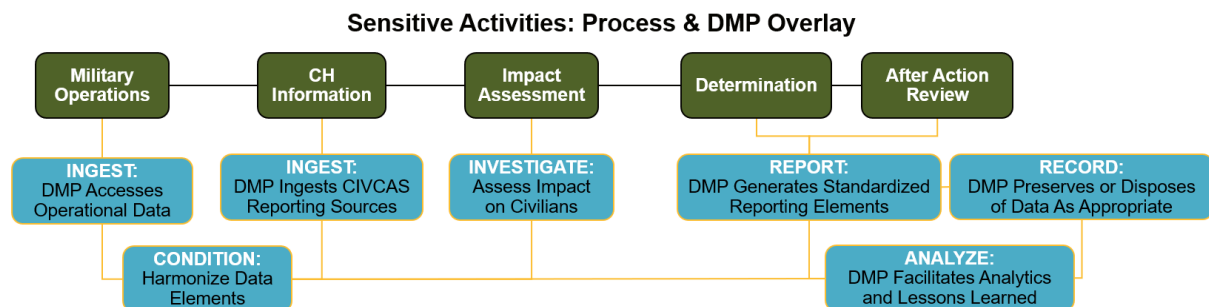


Figure C-6. Sensitive Activities Process & DMP Overlay

Appendix D. Detailed Information Requirements

Table D-1 depicts example information requirements for each vignette. These information requirements stem from user actions and inform DMP data requirements and technical requirements.

Table D-1. Detailed Information Requirements by Vignette and Key User

Vignette	Key User	User Action	Information Requirement
Targeting	CCMD	Perform CH assessment.	Create a CH assessment file, connecting to meta-data for inclusion as appropriate.
Targeting	CCMD	Record CIVCAS allegation.	Create an investigation/allegation file, connecting to meta-data for inclusion as appropriate.
Targeting	CCMD	Support CCMD response to CH incident.	Record findings and response, storing investigation-relevant data as appropriate.
Targeting	CP CoE	Produce and disseminate standardized reporting.	Access investigation and CH assessment metadata for inclusion in aggregated reporting.
Targeting	CP CoE	Identify lessons learned.	Access non-events and instances where no CIVCAS was found to enable unbiased statistics.
Targeting	CP CoE	Identify lessons learned.	Compare collateral damage estimates (CDEs) with sustained CIVCAS.
Targeting	CP CoE	Produce and disseminate standardized reporting.	Generate and report summary statistics about CH incidents, allegations, and responses.
Targeting	CP CoE	Produce and disseminate standardized reporting.	Generate standardized reports at various classification levels.
Targeting	CP CoE	Identify lessons learned.	Identify leading indicators and best practices to mitigate and prevent CIVCAS.
Targeting	CP CoE	Identify lessons learned.	Standardize data fields to enable cross CCMD data analysis.

Vignette	Key User	User Action	Information Requirement
Targeting	IO	Initiate and conduct an investigation.	Create an investigation/allegation file, connecting to meta-data for inclusion as appropriate.
Targeting	IO	Issue a CIVCAS determination.	Record findings and response, storing investigation-relevant data as appropriate.
Targeting	IO	Record CCAR progress.	Track progress and time to complete.
Troops in Contact	CCMD	Receives flagged incident.	Access relevant CH data.
Troops in Contact	CCMD	Document findings and support CCMD response.	Record findings and response, storing investigation-relevant data as appropriate.
Troops in Contact	IO	Initiate and conduct an investigation.	Create an investigation/allegation file, connecting to meta-data for inclusion as appropriate.
Troops in Contact	IO	Record investigation progress and results.	Record findings and response, storing investigation-relevant data as appropriate.
False Claim	CCMD	Initiate and conduct an investigation.	Create an investigation/allegation file, connecting to meta-data for inclusion as appropriate.
False Claim	CCMD	Generate standardized reporting.	Generate and report summary statistics about CH incidents, allegations, and responses.
False Claim	CCMD	Generate standardized reporting.	Generate standardized reports at various classification levels.
False Claim	CCMD	Document and support CCMD findings surrounding U.S. non-involvement.	Record findings and response, storing investigation-relevant data as appropriate.
False Claim	IO	Initiate and conduct an investigation.	Create an investigation/allegation file, connecting to meta-data for inclusion as appropriate.
False Claim	IO	Document and support CCMD findings surrounding U.S. non-involvement.	Record findings and response, storing investigation-relevant data as appropriate.
False Claim	P	Report CH claims via public access mechanism.	Collect public reports.
False Claim	P	Report CH claims via public access mechanism.	Distribute reports to appropriate authorities.
False Claim	P	Report CH claims via public access mechanism.	Provide a mechanism for the public to report CH information.
False Claim	P	Report CH claims via public access mechanism.	Retain information about number of reports, type, and outcomes.

Vignette	Key User	User Action	Information Requirement
Multinational Operation	CA	Distribute standardized reporting as appropriate.	Access standardized reports at various classification levels.
Multinational Operation	CCMD	Document findings and support CCMD response.	Access investigation and CH assessment meta-data for inclusion in aggregated reporting.
Multinational Operation	CP CoE	Produce and disseminate standardized reporting.	Access investigation and CH assessment meta-data for inclusion in aggregated reporting.
Multinational Operation	CP CoE	Produce and disseminate standardized reporting.	Generate and report summary statistics about CH incidents, allegations, and responses.
Multinational Operation	CP CoE	Produce and disseminate standardized reporting.	Generate standardized reports at various classification levels.
Multinational Operation	IO	Reference multinational partner data.	Access appropriate multinational partner meta-data for inclusion in aggregated reporting.
Multinational Operation	IO	Initiate and conduct an investigation.	Create an investigation/allegation file, connecting to meta-data for inclusion as appropriate.
Multinational Operation	IO	Generate standardized reporting.	Generate and report summary statistics about CH incidents, allegations, and responses.
Multinational Operation	IO	Generate standardized reporting.	Generate standardized reports at various classification levels.
Multinational Operation	IO	Document findings and support CCMD response.	Record findings and response, storing investigation-relevant data as appropriate.
Multinational Operation	IO	Document findings and support CCMD response.	Track investigation progress and time to complete.
Multinational Operation	O (Allies and Partners)	Provides access to multinational partner data.	Access appropriate multinational partner meta-data for inclusion in aggregated reporting.
Multinational Operation	P	Report CH claims via public access mechanism.	Collect public reports.
Multinational Operation	P	Report CH claims via public access mechanism.	Distribute reports to appropriate authorities.

Vignette	Key User	User Action	Information Requirement
Multinational Operation	P	Report CH claims via public access mechanism.	Provide a mechanism for the public to report CH information.
Multinational Operation	P	Report CH claims via public access mechanism.	Retain information about number of reports, type, and outcomes.
Sensitive Activities	CCMD	Conduct after action review.	Ensure that DMP schema, ontology, and documentation set standards for data—even outside of DMP.
Sensitive Activities	CCMD	Generate lessons learned and training.	Ensure that DMP schema, ontology, and documentation set standards for data—even outside of DMP.
Sensitive Activities	CCMD	Record operational data.	Ensure that DMP schema, ontology, and documentation set standards for data—even outside of DMP.
Sensitive Activities	IO	Conduct after action review.	Ensure that DMP schema, ontology, and documentation set standards for data—even outside of DMP.

Appendix E. Data Sources

IDA was provided a list of approximately 3,600 DoD data systems documented by DITPR. The IDA team triaged these systems to prioritize those that contained operational or intelligence information, and existing data platforms that aggregate data from a variety of systems. Table E-1 lists the 214 systems found to be in scope for the DMP aligned with vignettes. Table E-2 lists an additional 226 systems require further research for appropriate categorization.

Table E-1. Data Systems In Scope for DMP

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	ARMY AIRFIELD AUTOMATION SYSTEM 2.0	AAAS	ARMY	ASA(ALT) - PEO AVN Tactical	WMA-Command and Control (C2)	UNCLASS	X			X	
Engineering	AERO ADVISORIES SERVER (AAS) FOR THE AERO ADVISORIES AND NOTAMS TOOL (AANT)	AAS	USAF	ACC	WMA-Command and Control (C2)	SECRET	X			X	
Data	AVIATION DATA MANAGEMENT AND CONTROL SYSTEM	ADMACS	Navy	NAVAIR	WMA-Force Application (FA)	UNCLASS	X		X	X	
Data	ADVANA	ADVANA	CDAO		BMA	SECRET					
Logistics & Sustainment	AIRFIELD AUTOMATED SYSTEM	AFAS	USAF	AFMC	WMA-Logistics (L)	UNCLASS	X			X	
Operations	ADVANCED FIELD ARTILLERY TACTICAL DATA SYSTEM 6.8	AFATDS 6.8.	ARMY	ASA(ALT) - PEO C3T	WMA-Command and Control (C2)	SECRET	X	X			

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Logistics & Sustainment	AIR FORCE-GLOBAL ENTERPRISE TRACKING	AFGET	USAF	AFMC	BMA	UNCLASS	X		X	X	
Other	AIR FORCE GEOSPATIAL INFORMATION MANAGEMENT SYSTEM	AFGIMS	USAF	AFMC	BMA	UNCLASS	X		X	X	
Other	ARMY GEOSPATIAL ENTERPRISE GEOGLOBE	AGE GEOGLOBE	ARMY	USACE - [None]	WMA-Battlespace Awareness (BA)	UNCLASS	X	X	X	X	
Engineering	AVIATION AND MISSILE COMMAND (AMCOM) AMMUNITION TRACKING SYSTEM	AMCATS	ARMY	AMC - AMCOM - U.S. Army Aviation and Missile Command	BMA	SBU	X		X	X	
Engineering	AVIATION AND MISSILE COMMAND REPORTING AND DATA ANALYSIS WAREHOUSE	AMCOM RDAW	ARMY	AMC - AMCOM - U.S. Army Aviation and Missile Command	BMA	SBU					
Logistics & Sustainment	AVIATION MISSION PLANNING SYSTEM 7.7	AMPS 7.7	ARMY	ASA(ALT) - PEO AVN Tactical	WMA-Force Application (FA)	UNCLASS	X		X	X	
Other	AGILE MUNITIONS SUPPORT TOOL	AMST	USAF	AFMC	BMA	UNCLASS	X		X	X	

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	FACSFAC AIR CONTROL TRACKING SYSTEM (FACTS)	AN/FYK-39 FACTS	Navy	NAVAIR	WMA-Force Support (FS)		X		X	X	
Operations	AIR AND SPACE OPERATIONS CENTER-WEAPON SYSTEM 10.1	AOC-WS 10.1	USAF	ACC	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Intelligence	AIRBORNE RECONNAISSANCE LOW - MULTIFUNCTION (AN/ASQ-223)	ARL-M	ARMY	ASA(ALT) - PEO IEW&S PM SAI - Sensors Aerial Intelligence	WMA-Battlespace Awareness (BA)	SECRET	X	X			
Other	ARMY VANTAGE	ARMY VANTAGE	ARMY	ASA(ALT) - PEO EIS - Enterprise Information Systems	BMA	SECRET					
Other	ARMY VANTAGE-NIPRNET	ARMY VANTAGE-N	ARMY	ASA(ALT) - PEO EIS - Enterprise Information Systems	BMA	UNCLASS					
Logistics & Sustainment	AMMUNITION SUPPLY POINT MANAGEMENT SYSTEM	ASPMP	ARMY	AMC - ASC - U.S. Army Sustainment Command	BMA	UNCLASS		X	X		
Logistics & Sustainment	ALL WEAPONS INFORMATION SYSTEM	AWIS - SYSTEM LEVEL	DON	NAVAIR	BMA	SECRET	X		X		

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Logistics & Sustainment	BASE SUPPORT & EXPEDITIONARY PLANNING TOOL	BaS&E	USAF	AFMC	BMA	SECRET	X	X	X	X	
Security	BIOMETRICS AUTOMATED TOOLSET- ARMY	BAT-A V4.1	ARMY	ASA(ALT) - PEO IEW&S - PM Biometrics	WMA- Battlespace Awareness (BA)	SECRET		X			
Security	BIOMETRICS AUTOMATED TOOLSET- ARMY HANDHELD; TYPE II CRN STANDALONE	BAT-HH V1.2.4	ARMY	ASA(ALT) - PEO IEW&S - PM Biometrics	WMA- Battlespace Awareness (BA)	UNCLASS		X			
Operations	BATTLE CONTROL SYSTEM-FIXED INCREMENT 3	BCS-F Inc 3	USAF	ACC	WMA- Command and Control (C2)	SECRET	X	X	X	X	
Operations	BASE EXPEDITIONARY TARGETING SURVEILLANCE SYSTEM-COMBINED FAMILY OF SYSTEMS BLOCK II	BETSS-C FOS (BLOCK II)	ARMY	ASA(ALT) - PEO IEW&S PM TS - Terrestrial Sensors	WMA- Battlespace Awareness (BA)	SECRET	X	X			
Operations	BLUE FORCE TRACKING-1	BFT-1	ARMY	ASA(ALT) - PEO C3T	WMA- Command and Control (C2)	SBU	X	X	X	X	
Operations	BLUE FORCE TRACKING-2	BFT-2	ARMY	ASA(ALT) - PEO C3T	WMA- Command	SBU	X	X	X	X	

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
					and Control (C2)						
Security	BIOMETRIC IDENTITY INTELLIGENCE RESOURCE	BI2R	ARMY	INSCOM - NGIC - National Ground Intelligence Center	DIMA- Analysis and Production	TS	X	X	X		
Security	COMMAND, CONTROL, BATTLE MANAGEMENT AND COMMUNICATIONS 8.2	C2BMC S-8.2	MDA	BC	WMA- Protection (P)	SECRET	X		X	X	
Operations	COMMAND AND CONTROL OF INFORMATION ENVIRONMENT COLLABORATIVE MISSION MANAGER (C2IE-MM)	C2IE-MM	ARMY	USACE - [None]	WMA- Command and Control (C2)	SECRET					
Operations	COMMON AVIATION COMMAND AND CONTROL SYSTEM	CAC2S	USMC	USMC	WMA- Command and Control (C2)	SECRET	X			X	
Logistics & Sustainment	CHEMICAL ACCOUNTABILITY MANAGEMENT INFORMATION NETWORK	CAMIN	ARMY	AMC - CMA - Chemical Material Agency	BMA	UNCLASS			X		
Logistics & Sustainment	CONSOLIDATED AIR MOBILITY PLANNING SYSTEM	CAMPS	USTRANSCOM	HQ AMC	WMA- Logistics (L)	SBU	X		X	X	

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Logistics & Sustainment	CONSOLIDATED AIR MOBILITY PLANNING SYSTEM - C	CAMPS - C	USTRANSCOM	HQ AMC	WMA-Logistics (L)	SECRET	X		X	X	
Operations	COMBINED AIR AND SPACE OPERATIONS CENTER NELLIS	CAOC-N	USAF	ACC	WMA-Command and Control (C2)	SECRET	X				
Operations	CAOC-X	CAOC-X	USAF	ACC	WMA-Command and Control (C2)	SECRET	X			X	
Operations	CERBERUS LITE-SCOUT	CBL-S	ARMY	ASA(ALT) - PEO IEW&S PM TS - Terrestrial Sensors	WMA-Battlespace Awareness (BA)	SECRET		X			
Operations	COMBAT CAMERA SYSTEMS	CCS	USMC	USMC	WMA-Force Application (FA)	Other	X		X	X	
Operations	COMMAND AND CONTROL SYSTEM - CONSOLIDATED	CCS-C	USAF	USSF	WMA-Command and Control (C2)		X			X	
Security	CYBERSPACE DEFENSE ANALYSIS WEAPON SYSTEM	CDA WS	USAF	ACC	EIEMA-Core Enterprise Services	UNCLASS					X
Other	CROSS DOMAIN ENTERPRISE SERVICES	CDES	DISA	DBC ID5	EIEMA-Information Assurance	SECRET					

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	COOPERATIVE ENGAGEMENT CAPABILITY	CEC	Navy	NAVSEA	WMA-Protection (P)	SECRET	X				
Intelligence	COMMON GEOSPATIAL SERVER APPLICATIONS	CGSA	USMC		DIMA-Dissemination	SECRET	X		X	X	
Intelligence	COMMON GEOSPATIAL INTELLIGENCE WORKSTATION	CGW	USMC		DIMA-Analysis and Production	SECRET	X		X	X	
Intelligence	COMMON GEOSPATIAL INTELLIGENCE WORKSTATION-LITE-NIPRNET	CGW-L-N	USMC		DIMA-Exploitation	UNCLASS	X		X	X	
Intelligence	COMMON GEOSPATIAL INTELLIGENCE WORKSTATION - LITE - SIPRNET	CGW-L-S	USMC		DIMA-Exploitation	SECRET	X		X	X	
Security	CENTRALIZED INTEGRATED SYSTEM INTERNATIONAL LOGISTICS	CISIL	DSCA	DSADC	BMA	UNCLASS				X	
Logistics & Sustainment	COMMON LOGISTICS COMMAND AND CONTROL SYSTEM	CLC2S	USMC	USMC	BMA	UNCLASS	X	X		X	
Operations	COMPUTERIZED OPERATIONS MOVEMENT PLANNING AND STATUS SYSTEM	COMPASS	ARMY	FORSCOM - HQ FORSCOM	BMA	SECRET	X	X	X		

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Logistics & Sustainment	COLLABORATION PATHFINDER	CP	DLA	J64 EIS	EIEMA-Core Enterprise Services	UNCLASS		X			
Operations	CENTCOM PARTNER NETWORK - UNITED ARAB OF EMIRATES	CPN ARE	USCENTCOM		WMA-Command and Control (C2)	SECRET				X	
Operations	CENTCOM PARTNER NETWORK - BAHRAIN	CPN-BHR	USCENTCOM		WMA-Command and Control (C2)	SECRET				X	
Operations	CENTCOM PARTNER NETWORK - JORDAN	CPN-JOR	USCENTCOM		WMA-Command and Control (C2)	SECRET				X	
Operations	CENTCOM PARTNER NETWORK - KUWAIT	CPN-KWT	USCENTCOM		WMA-Command and Control (C2)	SECRET				X	
Operations	CENTCOM PARTNER NETWORK QATAR	CPN-QAT	USCENTCOM		WMA-Command and Control (C2)	SECRET				X	
Operations	CENTCOM PARTNER NETWORK - KINGDOM OF SAUDI ARABIA	CPN-SAU	USCENTCOM		WMA-Command and Control (C2)	SECRET				X	

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	CENTCOM PARTNER NETWORK VOICE AND VIDEO	CPN-USA	USCENTCOM		WMA-Command and Control (C2)	SECRET				X	
Operations	CENTCOM PARTNER NETWORK X	CPN-X	USCENTCOM		EIEMA-Core Enterprise Services	SECRET				X	
Operations	COUNTER ROCKET ARTILLERY AND MORTAR COMMAND & CONTROL/FORWARD AREA AIR DEFENSE COMMAND & CONTROL	CRAMC2/FAADC2	ARMY	ASA(ALT) - PEO MS Tactical	WMA-Protection (P)	SECRET		X	X		
Operations	CENTER SCHEDULING ENTERPRISE	CSE	USAF	AFMC	WMA-Command and Control (C2)	SBU	X		X	X	
Other	C2 URGENT RESPONSE ENVIRONMENT	CURE	USAF	AFMC	WMA-Corporate Management and Support (CMS)	UNCLASS					
Data	DEPLOY TO REDEPLOY AND RETROGRADE ANALYTICAL TOOL	D2RRAT	ARMY	HQDA G3 - SO	BMA	SECRET	X	X	X	X	
Data	DEPLOY TO REDEPLOY AND RETROGRADE DATA LAKE	D2RRDL	ARMY	HQDA G3 - SO	BMA	SECRET	X	X	X	X	

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Engineering	DOD AERONAUTICAL INFORMATION PORTAL	DAIP	USAF	AFMC	EIEMA-Computing Infrastructure	UNCLASS	X			X	
Operations	DEEP SPACE ADVANCED RADAR CAPABILITY	DARC	USAF	USSF	DIMA-Enterprise Information Technology (Aligns with EIEMA)	SECRET					X
Operations	DELIBERATE AND CRISIS ACTION PLANNING AND EXECUTION SEGMENTS C2	DCAPES C2	USAF	ACC	WMA-Command and Control (C2)	SECRET	X	X	X	X	
Operations	DISTRIBUTED COMMON GROUND SYSTEM - ARMY FIXED SITE FAMILY OF SYSTEMS	DCGS-A FIXED SITE FOS	ARMY	ASA(ALT) - PEO IEW&S PM DCGS-A - Distributed Common Ground System - Army	WMA-Battlespace Awareness (BA)	Other	X	X	X	X	X
Operations	DISTRIBUTED COMMON GROUND SYSTEMS - ARMY FAMILY OF SYSTEM	DCGS-A FOS	ARMY	ASA(ALT) - PEO IEW&S PM DCGS-A - Distributed Common Ground System - Army	WMA-Battlespace Awareness (BA)	Other	X	X	X	X	X

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	DISTRIBUTED COMMON GROUND SYSTEM - ARMY VERSION 3.2.5	DCGS-A V3.2.5	ARMY	ASA(ALT) - PEO IEW&S PM DCGS-A - Distributed Common Ground System - Army	WMA- Battlespace Awareness (BA)	UNCLASS	X	X	X	X	X
Operations	DISTRIBUTED COMMON GROUND SYSTEM - ARMY VERSION 3.2.5	DCGS-A V3.2.5	ARMY	ASA(ALT) - PEO IEW&S PM DCGS-A - Distributed Common Ground System - Army	WMA- Battlespace Awareness (BA)	SECRET	X	X	X	X	X
Operations	DISTRIBUTED COMMON GROUND SYSTEM - ARMY VERSION 3.2.5	DCGS-A V3.2.5	ARMY	ASA(ALT) - PEO IEW&S PM DCGS-A - Distributed Common Ground System - Army	WMA- Battlespace Awareness (BA)	TS	X	X	X	X	X
Intelligence	DISTRIBUTED COMMON GROUND/SURFACE SYSTEM - MARINE CORPS	DCGS-MC	USMC	USMC	DIMA- Dissemination	SECRET	X	X	X	X	X
Intelligence	DISTRIBUTED COMMON GROUND/SURFACE SYSTEM-MARINE CORPS ALL SOURCE	DCGS-MC ALL SOURCE	USMC		DIMA- Analysis and Production	SECRET	X	X	X	X	X

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Intelligence	DISTRIBUTED COMMON GROUND/SURFACE SYSTEM-MARINE CORPS GEOSPATIAL INTELLIGENCE	DCGS-MC GEOINT	USMC		DIMA-Analysis and Production	SECRET	X	X	X	X	X
Operations	DISTRIBUTED COMMON GROUND SYSTEM - NAVY INCREMENT 2	DCGS-N INC 2	Navy	SPAWAR	WMA-Battlespace Awareness (BA)	SECRET	X	X	X	X	X
Operations	DISTRIBUTED COMMON GROUND SYSTEM - NAVY	DCGS-N INC I	Navy	SPAWAR	WMA-Battlespace Awareness (BA)	SECRET	X	X	X	X	X
Engineering	DIGITAL CAMERA RECIEVING STATION	DCRS	Navy	NAVAIR	DIMA-Dissemination	SECRET	X				
Data	ENTERPRISE DATA WAREHOUSE	DIA-EDW	DIA	CFO	BMA	TS					X
Intelligence	INTELINK RESOURCE MANAGEMENT INFORMATION SYSTEMS	DIA-IRMIS	DIA	CFO	BMA	TS					
Intelligence	INTELINK RESOURCE MANAGEMENT INFORMATION - FINANCIAL INTEGRATION	DIA-IRMIS FI	DIA	CFO	BMA	TS					
Operations	DEPLOYABLE MISSION SUPPORT SYSTEM	DMSS	USMC		WMA-Force Application (FA)						X

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Security	DOD AUTOMATED BIOMETRICS IDENTIFICATION SYSTEM DISASTER RECOVERY SYSTEM (DRS)	DOD ABIS DRS V1.3	ARMY	ASA(ALT) - PEO IEW&S - PM Biometrics	WMA- Battlespace Awareness (BA)	UNCLASS	X	X			
Security	DOD AUTOMATED BIOMETRICS IDENTIFICATION SYSTEM OPERATIONAL ENVIRONMENT V1.3	DOD ABIS OE V1.3	ARMY	ASA(ALT) - PEO IEW&S - PM Biometrics	WMA- Battlespace Awareness (BA)	UNCLASS	X	X			
Other	DEPARTMENT OF DEFENSE 365 - SECRET	DoD365-SEC	DISA	DBC SD3	DIMA- Enterprise Information Technology (Aligns with EIEMA)	SECRET					
Logistics & Sustainment	DEFENSE PROPERTY ACCOUNTABILITY SYSTEM	DPAS	DLA	J62H	BMA	UNCLASS	X	X	X		
Other	DPCLTD COMPLIANCE AND REPORTING TOOL	DPCLTD CART	DA&M	Office of the Assistant to the Secretary of Defense (Privacy, Civil Liberties, and Transparency)	BMA	UNCLASS			X		
Operations	DEPARTMENT OF DEFENSE (DOD) PRIVACY INFORMATION	DPIMS	DISA	DCSC-SD2	EIEMA-Core Enterprise Services	UNCLASS			X		

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
	MANAGEMENT SYSTEM (DPIMS)										
Security	DEFENSE SECURITY ASSISTANCE MANAGEMENT SYSTEM	DSAMS	DSCA	DSADC	BMA	UNCLASS				X	
Data	ENTERPRISE DATA WAREHOUSE	EDW	DLA	J62K	EIEMA-Core Enterprise Services	UNCLASS					
Data	ENTERPRISE DATA WAREHOUSE	EDW	Navy	NAVSEA	EIEMA-Computing Infrastructure	UNCLASS					
Security	EXPEDITIONARY FORENSIC EXPLOITATION CAPABILITY	EFEC	USMC		WMA-Battlespace Awareness (BA)		X	X	X		
Other	ELECTRONIC FREEDOM OF INFORMATION ACT	e-FOIA	USAF	ACC	EIEMA-Core Enterprise Services	UNCLASS	X	X	X	X	X
Other	EHQMC SHAREPOINT	eHQMC	USMC		EIEMA-Core Enterprise Services	UNCLASS					
Other	ENTERPRISE KNOWLEDGE REPOSITORY	EKR	ARMY	OBT - [None]	BMA	UNCLASS					
Operations	ENHANCED MEDIUM ALTITUDE RECONNAISSANCE AND SURVEILLANCE SYSTEM	EMARSS	ARMY	ASA(ALT) - PEO IEW&S PM SAI - Sensors Aerial Intelligence	WMA-Battlespace Awareness (BA)	TS					X

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Intelligence	(EMARSS-S)ENHANCED MEDIUM ALTITUDE RECONNAISSANCE AND SURVEILLANCE SYSTEM	EMORYTINSEL-S	ARMY	ASA(ALT) - PEO IEW&S PM SAI - Sensors Aerial Intelligence	WMA-Battlespace Awareness (BA)	SECRET	X	X	X		
Operations	ENHANCED POSITION LOCATION REPORTING SYSTEM	EPLRS	Navy	SPAWAR	WMA-Command and Control (C2)	UNCLASS	X	X	X	X	X
Operations	ENHANCED POSITION LOCATION REPORTING SYSTEM SIS TYPE III	EPLRS SIS TYPE III	ARMY	ASA(ALT) - PEO C3T	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Operations	ELECTRONIC WARFARE PLANNING AND MANAGEMENT TOOL	EWPM T V1.3	ARMY	ASA(ALT) - PEO IEW&S PM EW&S - Electronic Warfare & Cyber	WMA-Battlespace Awareness (BA)	SECRET	X	X			X
Intelligence	(EMARSS-G)ENHANCED MEDIUM ALTITUDE RECONNAISSANCE AND SURVEILLANCE SYSTEM	EXITQUICKLY-G	ARMY	ASA(ALT) - PEO IEW&S PM SAI - Sensors Aerial Intelligence	WMA-Battlespace Awareness (BA)	SECRET	X	X	X		
Intelligence	(EMARSS-M)ENHANCED MEDIUM ALTITUDE RECONNAISSANCE AND SURVEILLANCE SYSTEM	EXITQUICKLY-M	ARMY	ASA(ALT) - PEO IEW&S PM SAI - Sensors Aerial Intelligence	WMA-Battlespace Awareness (BA)	SECRET	X	X	X		

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Intelligence	(EMARSS-V)ENHANCED MEDIUM ALTITUDE RECONNAISSANCE AND SURVEILLANCE SYSTEM	EXITQUICKLY-V	ARMY	ASA(ALT) - PEO IEW&S PM SAI - Sensors Aerial Intelligence	WMA-Battlespace Awareness (BA)	SECRET	X	X	X		
Logistics & Sustainment	FLIGHT INFORMATION SCHEDULING AND TRACKING	FIST	Navy	NAVAIR	EIEMA-Core Enterprise Services	UNCLASS	X	X	X	X	
Engineering	FLIGHT CLEARANCE PROCESSING SYSTEMS	FLIGHT CLEARANCE	Navy	NAVAIR	EIEMA-Core Enterprise Services	UNCLASS	X	X	X	X	
Operations	FORCE MANAGEMENT SYSTEM (FMS)	FMS	ARMY	HQDA G3 - FM	BMA	SBU	X	X	X		
Operations	FORCE MANAGEMENT SYSTEM (CLASSIFIED)	FMS(C)	ARMY	HQDA G3 - FM	BMA	SECRET	X	X	X		
Acquisition	FOREIGN MILITARY SALES DATA DISTRIBUTION SYSTEM	FMSDDS	USAF	ACC	WMA-Force Support (FS)	SECRET				X	
Operations	FORCE MANAGEMENT SYSTEM WEB SITE	FMSWEB	ARMY	HQDA G3 - FM	BMA	SBU	X	X	X		
Personnel	FORCE RISK REDUCTION	FR2	USD(P&R)	FSOH	WMA-Force Support (FS)	SBU					
Operations	G2 OPERATIONAL ENVIRONMENT MISSION SYSTEM - SECURE INTERNET PROTOCOL ROUTER	G2 OEMS - SIPR	ARMY	TRADOC - HQ - TRADOC HQ	WMA-Battlespace Awareness (BA)	SECRET					

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	GLOBAL COMMAND AND CONTROL SYSTEM/PENTAGON	GCCS - J/PENTAGON	DISA	OPC FC	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Operations	GLOBAL COMMAND AND CONTROL SYSTEM AIR FORCE GLOBAL RELEASE	GCCS-AF_GR	USAF	ACC	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Operations	GLOBAL COMMAND AND CONTROL SYSTEM - JOINT 6.0	GCCS-J 6.0	DISA	DCSC SD4	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Operations	GLOBAL COMMAND AND CONTROL SYSTEM - JOINT CLOUD	GCCS-J Cloud	DISA	SD4	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Operations	GLOBAL COMMAND AND CONTROL SYSTEM - MARITIME	GCCS-M	Navy	SPAWAR	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Operations	GLOBAL COMMAND AND CONTROL SYSTEM - TACTICAL COMBAT OPERATIONS (GCCS-TCO)	GCCS-TCO	USMC	USMC	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Logistics & Sustainment	GLOBAL COMBAT SUPPORT SYSTEM - ARMY INCREMENT 1	GCSS-A INC 1	ARMY	HQDA G4 - G4 - PEO EIS PM GCSS-ARMY	BMA	UNCLASS	X	X	X	X	X

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Logistics & Sustainment	GLOBAL COMBAT SUPPORT SYSTEM - ARMY INCREMENT 2	GCSS-A INC 2	ARMY	HQDA G4 - G4 - PEO EIS PM GCSS-ARMY	BMA	UNCLASS	X	X	X	X	X
Logistics & Sustainment	GLOBAL COMBAT SUPPORT SYSTEM-MARINE CORPS/LOGISTICS CHAIN MANAGEMENT	GCSS-MC/LCM	USMC	USMC	BMA	UNCLASS	X	X	X	X	X
Data	GRAPHICAL DATA FUSION SYSTEM (GDFS)	GDFS	Navy	SPAWAR	WMA-Battlespace Awareness (BA)		X	X	X	X	
Operations	GLOBAL DECISION SUPPORT SYSTEM	GDSS	USTRANSCOM	HQ AMC	WMA-Command and Control (C2)	SBU			X		
Logistics & Sustainment	GLOBAL DECISION SUPPORT SYSTEM - C	GDSS - C	USTRANSCOM	HQ AMC	WMA-Logistics (L)	SECRET			X		
Operations	GLOBAL ELECTROMAGNETIC SPECTRUM INFORMATION SYSTEM - CLASSIFIED	GEMSIS-C	DISA	DBC DSO	EIEMA-Core Enterprise Services	SECRET					X
Operations	GLOBAL ELECTROMAGNETIC SPECTRUM INFORMATION - UNCLASSIFIED	GEMSIS-U	DISA	DBC DSO	EIEMA-Core Enterprise Services	UNCLASS					X

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	GLOBAL POSITIONING SYSTEM (GPS)-BASED POSITIONING, NAVIGATION, AND TIMING SERVICE	GPNTS	Navy	SPAWAR	WMA-Net Centric (NC)	Other	X	X	X	X	X
Operations	GPS - MASTER CONTROL STATION/ALTERNATE MASTER CONTROL STATION/REMOTE STATION (MONITORING STATION/GROUND ANTENNA)	GPS - MCS/AMCS/RS (MS/GA)	USAF	USSF	WMA-Battlespace Awareness (BA)	SECRET	X	X	X	X	X
Operations	GLOBAL POSITIONING SYSTEM BLOCK III INCREMENT A	GPS IIIA	USAF	USSF	WMA-Battlespace Awareness (BA)		X	X	X	X	X
Operations	GLOBAL POSITIONING SYSTEM INFORMATION NETWORK	GPS-GIN	USAF	USSF	WMA-Net Centric (NC)	SECRET	X	X	X	X	X
Operations	GLOBAL POSITIONING SYSTEMS INTEGRATED CORRELATION AND DISPLAY SYSTEM BUILD 6	GPS-ICADS-Build 6	USAF	USSF	WMA-Battlespace Awareness (BA)		X	X	X	X	X
Logistics & Sustainment	GPS - INTEGRATED MISSION OPERATIONS SUPPORT CENTER	GPS-IMOSC	USAF	USSF	WMA-Battlespace Awareness (BA)		X	X	X	X	X

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	GLOBAL POSITIONING SYSTEMS NEXT GENERATION OPERATIONAL CONTROL SEGMENT MASTER CONTROL STATION, ALTERNATE MASTER CONTROL STATION, AND REMOTE SITES	GPS-OCX-MARS	USAF	USSF	WMA-Command and Control (C2)		X	X	X	X	X
Operations	GPS - OPERATIONAL SUPPORT SYSTEM	GPS-OSS	USAF	USSF	WMA-Battlespace Awareness (BA)		X	X	X	X	X
Operations	GLOBAL SENSOR INTEGRATION ON NETWORKS MISSILE WARNING NETSERVER	GSIN MWNS	USAF	USSF	WMA-Command and Control (C2)	SECRET	X		X		
Logistics & Sustainment	HAZARDOUS INVENTORY CONTROL SYSTEM WINDOWS	HICSWIN	Navy	NAVSUP	BMA	UNCLASS			X		
Operations	CVN-68 NIMITZ CLASS HULL, MECHANICAL AND ELECTRICAL MACHINERY CONTROL AND MONITORING SYSTEMS	HM&E MCMS	Navy	NAVSEA	WMA-Force Application (FA)				X		
Logistics & Sustainment	HAZARDOUS MATERIAL MANAGEMENT SYSTEM	HMMS	DLA	J62H	BMA	SBU			X		

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	HAZARDOUS WEATHER DETECTION AND DISPLAY CAPABILITY	HWDDC	Navy	SPAWAR	WMA-Battlespace Awareness (BA)	SECRET					
Operations	COMPREHENSIVE COLLABORATIVE COMMAND AND CONTROL MISSION APPLICATION PLATFORM	I CORPS - C4MAP/VJOC	ARMY	FORSCOM - I Corps	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Data	INTERCONTINENTAL BALLISTIC MISSILE INTEGRATED DATA ENVIRONMENT	ICBM IDE	USAF	AFGSC	WMA-Protection (P)	UNCLASS	X				
Security	IDENTITY DOMINANCE SYSTEM-MARINE CORPS	IDS-MC	USMC	USMC	DIMA-Collection	UNCLASS	X	X	X		
Security	IDENTITY DOMINANCE SYSTEM - MARINE CORPS INC 2	IDS-MC Inc 2	USMC		DIMA-Collection	UNCLASS	X	X	X		
Operations	IDENTIFICATION FRIEND OR FOE KIV-77	IFF 77	USAF	ACC	WMA-Force Support (FS)		X	X	X		
Operations	IDENTIFICATION FRIEND OR FOE KIV-78	IFF 78	USAF	ACC	WMA-Force Support (FS)		X	X	X		
Data	INTEGRATED DATA ENVIRONMENT/GLOBAL TRANSPORTATION NETWORK CONVERGENCE	IGC	USTRANSCOM	USTRANSCOM	WMA-Command and Control (C2)	SBU					

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Data	INTEGRATED DATA ENVIRONMENT/GLOBAL TRANSPORTATION NETWORK CONVERGENCE - C	IGC - C	USTRANSCOM	USTRANSCOM	WMA-Command and Control (C2)	SECRET					
Logistics & Sustainment	INTEGRATED GLOBAL UID ENTERPRISE SOLUTION	I-GUIDES	USMC	USMC	BMA						
Intelligence	INTELLIGENCE KNOWLEDGE NETWORK	IKN	ARMY	TRADOC - ICoe - Intelligence Center of Excellence	EIEMA-Core Enterprise Services	UNCLASS					
Intelligence	INTELLIGENCE KNOWLEDGE NETWORK - SECRET	IKN-S	ARMY	TRADOC - ICoe - Intelligence Center of Excellence	EIEMA-Core Enterprise Services	SECRET					
Data	INTEGRATED MISSILE DATA BASE	IMDB	USAF	AFGSC	BMA	UNCLASS	X				
Intelligence	INFORMATION OPERATIONS PLATFORM	IOP	USAF	ACC	EIEMA-Information Assurance	SECRET					X
Intelligence	INTELLIGENCE PRODUCTION AND DISSEMINATION SYSTEM	IPDS	ARMY	INSCOM - NGIC - National Ground Intelligence Center	EIEMA-Core Enterprise Services	SECRET	X		X		X

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Logistics & Sustainment	INTEGRATED STRATEGIC PLANNING AND ANALYSIS NETWORK (ISPAN) PROGRAM	ISPAN	USSTRATCOM		WMA-Command and Control (C2)	TS					X
Engineering	JOINT ACQUISITION CHEMICAL BIOLOGICAL RADIOLOGICAL NUCLEAR KNOWLEDGE SYSTEM	JACKS	ARMY	ASA(ALT) - JPEO-CBD - Joint PEO Chemical and Biological Defense	BMA				X		
Operations	JOINT AUTOMATED DEEP OPERATIONS COORDINATION SYSTEM V2.0	JADOCS V2.0	ARMY	ASA(ALT) - PEO C3T	WMA-Command and Control (C2)	SECRET	X	X	X		
Operations	JOINT AIR DEFENSE SYSTEMS INTEGRATOR	JADSI	USAF	ACC	WMA-Command and Control (C2)	SECRET	X	X	X		
Engineering	JOINT COMMON FOUNDATION (AWS)	JCF-AWS	CDAO		EIEMA-Computing Infrastructure	UNCLASS					
Engineering	JOINT COMMON FOUNDATION-AZURE	JCF-AZURE	CDAO		EIEMA-Computing Infrastructure						
Logistics & Sustainment	JOINT EQUIPMENT CHARACTERISTICS DATABASE - U	JECD - U	USTRANSCOM	SDDC	EIEMA-Computing Infrastructure	SBU	X	X	X		

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Engineering	JOINT EFFECTS MODEL	JEM	ARMY	ASA(ALT) - JPEO-CBD - Joint PEO Chemical and Biological Defense	WMA-Protection (P)	SECRET	X	X	X	X	
Engineering	JOINT EFFECTS MODEL	JEM	ARMY	ASA(ALT) - JPEO-CBD - Joint PEO Chemical and Biological Defense	WMA-Protection (P)	SBU	X	X	X	X	
Operations	JOINT HIGH SPEED VESSEL ELECTRONIC CHART DISPLAY AND INFORMATION SYSTEM	JHSV ECDIS	Navy	NAVSEA	WMA-Command and Control (C2)	Other	X		X	X	
Personnel	JOINT LESSONS LEARNED INFORMATION SYSTEM - SIPRNET	JLLIS-S	JOINT STAFF	J7	WMA-Force Support (FS)	SECRET					
Personnel	JOINT LESSONS LEARNED INFORMATION SYSTEM - UNCLASS	JLLIS-U	JOINT STAFF	J7	WMA-Force Support (FS)	UNCLASS					
Operations	JOINT MISSION PLANNING SYSTEM	JMPS	Navy	NAVAIR	WMA-Command and Control (C2)	SECRET	X	X	X	X	X

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	JOINT MISSION PLANNING SYSTEM	JMPS	USAF	ACC	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Operations	JSPOC MISSION SYSTEM VERSION	JMS v	USAF	USSF	WMA-Battlespace Awareness (BA)	TS					X
Operations	JPES JOINT OPERATION PLANNING AND EXECUTION SYSTEM (TYPE ACCREDITATION)	JOPEs	DISA	DCSC-SD4	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Operations	JOINT OPERATION PLANNING AND EXECUTION SYSTEM / PENTAGON	JOPEs / PENTAGON	DISA	OPC FC	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Operations	JOINT PRECISION AIR DROP SYSTEM SIS TIII	JPADS	ARMY	ASA(ALT) - PEO CS&CSS PM E2S2	WMA-Logistics (L)	UNCLASS				X	X
Operations	JOINT PRECISION AIRDROP SYSTEM-MISSION PLANNER	JPADS-MP	USAF	ACC	WMA-Command and Control (C2)	UNCLASS				X	X
Requirements	JOINT STAFF ANALYTICAL SUITE	JSAS	JOINT STAFF	J8	WMA-Force Support (FS)	Other					
Operations	JOINT TACTICAL COMMON OPERATIONAL PICTURE WORKSTATION 1.X.X.X	JTCW 1.X.X.X	USMC	USMC	WMA-Command and Control (C2)	SECRET	X	X	X	X	X

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Engineering	JOINT TECHNICAL DATA INTEGRATION	JTDI	Navy	NAVAIR	BMA	UNCLASS					
Operations	JOINT WARNING & REPORTING NETWORK	JWARN	ARMY	ASA(ALT) - JPEO-CBD - Joint PEO Chemical and Biological Defense	WMA-Protection (P)	SECRET	X		X	X	X
Operations	JOINT WARNING & REPORTING NETWORK	JWARN	ARMY	ASA(ALT) - JPEO-CBD - Joint PEO Chemical and Biological Defense	WMA-Protection (P)	UNCLASS	X		X	X	X
Security	KEY MANAGEMENT INFRASTRUCTURE	KMI	NSA		EIEMA-Information Assurance	SECRET					X
Security	MISSION ASSURANCE DECISION SUPPORT SYSTEM	MADSS	DON	DBC ID	EIEMA-Information Assurance	SECRET					
Security	MISSION ASSURANCE RISK MANAGEMENT SYSTEM	MARMS	DTRA		WMA-Protection (P)	SECRET					
Security	MARINE CORPS CRITICAL ASSET MANAGEMENT SYSTEM	MCCAMS	USMC	USMC	WMA-Protection (P)	SECRET	X	X	X	X	
Intelligence	MARINE CORPS COMMON INTELLIGENCE SERVER	MCCIS	USMC	USMC	DIMA-Analysis and Production	SECRET	X	X	X	X	X

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Other	MCIPAC GIS	MCIPAC GIS	USMC		BMA	UNCLASS	X	X	X	X	X
Engineering	MARINE CORPS PLATFORM INTEGRATION CENTER	MCPIC	USMC	USMC	BMA	UNCLASS					
Operations	MOBILIZATION DEPLOYMENT INFORMATION SYSTEM	MDIS	ARMY	HQDA G3 - OD	BMA	SECRET					
Logistics & Sustainment	MAPPING ENTERPRISE BUSINESS SYSTEM	MEBS	DLA	J62H	BMA	UNCLASS					
Intelligence	MILITARY INTELLIGENCE ACTIVE DIRECTORY NIPRNET FOREST - INSCOM - CCF	MIAD NIPRNET FOREST - INSCOM - CCF	ARMY	INSCOM - CCF - Central Clearance Facility	EIEMA-Core Enterprise Services	UNCLASS					
Intelligence	MILITARY INTELLIGENCE ACTIVE DIRECTORY SIPRNET FOREST - INSCOM - CCF	MIAD SIPRNET FOREST - INSCOM - CCF	ARMY	INSCOM - CCF - Central Clearance Facility	EIEMA-Core Enterprise Services	SECRET					
Logistics & Sustainment	MOBILITY INVENTORY CONTROL ACCOUNTABILITY SYSTEM WEB	MICAS WEB	ARMY	AMC - TACOM - U.S. Army Tank-Automotive and Armaments Command	BMA	UNCLASS	X	X	X	X	
Logistics & Sustainment	MUNITIONS ITEMS DISPOSITION ACTION SYSTEM	MIDAS	ARMY	AMC - JMC - U.S. Army Joint Munitions Command	BMA	UNCLASS	X	X	X	X	

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	FRIENDLY FORCE TRACKING MISSION MANAGEMENT CENTER - SECRET	MMC-S	ARMY	SMDC - [None]	WMA-Command and Control (C2)	SECRET	X	X	X	X	X
Operations	FORCE TRACKING MISSION MANAGEMENT CENTER - UNCLASSIFIED	MMC-U	ARMY	SMDC - [None]	WMA-Command and Control (C2)	UNCLASS	X	X	X	X	X
Logistics & Sustainment	MISSION PARTNER GATEWAY - EXTENDED	MPGW-X	USINDOPACOM		WMA-Command and Control (C2)					X	
Intelligence	MAVEN SMART SYSTEM	MSS	USD(I)	MCIA	WMA-Battlespace Awareness (BA)	SECRET					
Operations	MARITIME TACTICAL COMMAND AND CONTROL	MTC2	Navy	SPAWAR	WMA-Command and Control (C2)	SECRET	X		X		
Logistics & Sustainment	MUNITIONS TRANSPORTATION MANAGEMENT SYSTEM	MTMS	ARMY	AMC - JMC - U.S. Army Joint Munitions Command	BMA	UNCLASS	X	X	X	X	
Operations	COMMAND AND CONTROL OFFICIAL INFORMATION EXCHANGE (C2OIX)	NAVMACS II / SUBSMS AN/SYQ-28(V)	Navy	SPAWAR	WMA-Net Centric (NC)	SECRET			X		

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
	AFLOAT LEGACY (SUBSURFACE)										
Security	NAVY CYBER SITUATIONAL AWARENESS	NCSA	Navy	SPAWAR	WMA-Net Centric (NC)	SECRET					X
Data	NAVY DATA ENVIRONMENT	NDE	Navy	NAVSEA	BMA	UNCLASS					
Data	NAVY DATA PLATFORM	NDP	Navy		EIEMA-Core Enterprise Services	UNCLASS					
Logistics & Sustainment	NATIONAL LEVEL AMMUNITION CAPABILITY	NLAC	ARMY	HQDA G4 - [None]	BMA	UNCLASS	X		X		
Logistics & Sustainment	NATIONAL LEVEL AMMUNITION CAPABILITY - SIPRNET	NLAC-SIPR	ARMY	HQDA G4 - [None]	BMA	SECRET	X		X		
Personnel	NAVY READINESS REPORTING ENTERPRISE - CLASSIFIED	NRRE-C	Navy	USFFC	WMA-Force Support (FS)	SECRET		X			
Personnel	NAVY READINESS REPORTING ENTERPRISE - UNCLASSIFIED	NRRE-U	Navy	USFFC	WMA-Force Support (FS)	UNCLASS		X			

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Operations	NEAR REAL TIME IDENTITY OPERATION	NRTIO	ARMY	ASA(ALT) - PEO IEW&S - PM Biometrics	WMA-Battlespace Awareness (BA)	UNCLASS	X	X	X		X
Intelligence	NGIC SIGNATURES LABORATORY	NSL	ARMY	INSCOM - NGIC - National Ground Intelligence Center	DIMA-Collection	SECRET	X	X	X	X	X
Security	NEXT GENERATION BIOMETRICS CAPABILITIES COLLECTION	NXGBCC	ARMY	ASA(ALT) - PEO IEW&S - PM Biometrics	WMA-Battlespace Awareness (BA)	UNCLASS	X	X	X		X
Operations	ORION DECISION SUPPORT PLATFORM PRODUCTION	ODSP/P	JOINT STAFF	J35	WMA-Command and Control (C2)	SECRET					
Security	OVERSEAS HUMANITARIAN ASSISTANCE SHARED INFORMATION SYSTEM	OHASIS	DSCA		BMA	UNCLASS				X	
Logistics & Sustainment	ORDNANCE INFORMATION SYSTEM	OIS	Navy	NAVSUP	BMA	SECRET	X	X	X		
Other	PUBLIC AFFAIRS DMZ APPLICATIONS	PADMZ	ASD(PA)		EIEMA-Computing Infrastructure				X	X	

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification	Targeting Vignette	Troops in Contact Vignette	False Claim Vignette	Multinational Operation Vignette	Sensitive Activities Vignette
Other	PUBLIC AFFAIRS INFORMATION REVIEW SYSTEM	PAIRS	USAF	HAF	BMA	UNCLASS			X	X	
Other	PUBLIC AFFAIRS SYSTEMS	PAS	USMC	USMC	WMA-Force Application (FA)	UNCLASS			X	X	
Intelligence	PALANTIR DEFENSE SUITE	PDS	USMC		DIMA-Analysis and Production	SECRET					
Operations	PERSISTENT SURVEILLANCE AND DISSEMINATION SYSTEM OF SYSTEMS	PSDS2	ARMY	ASA(ALT) - PEO IEW&S PM TS - Terrestrial Sensors	WMA-Battlespace Awareness (BA)	SECRET	X		X		
Security	PHYSICAL SECURITY INTEGRATION FRAMEWORK INTERCONNECTION CAPABILITY SUITE	PSIF ICS	ARMY	ASA(ALT) - JPEO-CBD - Joint PEO Chemical and Biological Defense	WMA-Protection (P)	Other		X			

Table E-2. Data Systems Requiring Additional Research to Determine DMP Relevance

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Operations	618 AIR OPERATIONS CENTER	618 AOC	USTRANSCOM	HQ AMC	WMA-Logistics (L)	SBU
Operations	618 AIR OPERATIONS CENTER - C	618 AOC - C	USTRANSCOM	HQ AMC	WMA-Logistics (L)	SECRET

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Operations	ASSAULT AMPHIBIOUS VEHICLE COMMAND VARIANT MODEL 7A1	AAVC7A1	USMC	USMC	WMA-Command and Control (C2)	SECRET
Logistics & Sustainment	AIRCRAFT NOTEBOOK	ACN	ARMY	ASA(ALT) - PEO EIS - Enterprise Information Systems	BMA	UNCLASS
Logistics & Sustainment	AIRCRAFT DELIVERY INFORMATION SYSTEM	ADIS	USAF	ACC	WMA-Force Application (FA)	UNCLASS
Data	AVIATION DATA WAREHOUSE	ADW	Navy	COMPACFLT	WMA-Force Support (FS)	SECRET
Operations	AEGIS BALLISTIC MISSILE DEFENSE SYSTEM 3.6.1	AEGIS 3.6.1	MDA	AB	WMA-Protection (P)	SECRET
Operations	AEGIS BALLISTIC MISSILE DEFENSE SYSTEM 4.X	AEGIS BMD 4.X	MDA	AB	WMA-Protection (P)	SECRET
Logistics & Sustainment	AMMUNITION ENTERPRISE PORTAL (ME.SPACE)	AEP-JPEO A&A	ARMY	ASA(ALT) - Joint PEO Armaments & Ammunition (JPEO A&A)	BMA	UNCLASS
Other	ARMY ENTERPRISE SYSTEMS INTEGRATION PROGRAM	AESIP	ARMY	HQDA G4 - G4 - PEO EIS PL AESIP HUB	BMA	SBU
Requirements	AUTOMATED FORCES FOR	AFF	JOINT STAFF	J8	WMA-Force Support (FS)	SECRET
Logistics & Sustainment	AGING FLEET INTEGRITY AND RELIABILITY MANAGEMENT SYSTEM	AFIRM	USAF	AFMC	BMA	UNCLASS
Logistics & Sustainment	AGING FLEET INTEGRITY AND RELIABILITY MANAGEMENT MULTI-PLATFORM	AFIRM-M	USAF	AFMC	BMA	UNCLASS
Intelligence	HQ AFPC INTELLIGENT CONTACT MANAGEMENT SYSTEM	AFPC-ICMS	USAF	AF/A1	EIEMA-Computing Infrastructure	UNCLASS
Logistics & Sustainment	AFRC BASING & LOGISTICS GEOSPATIAL INFORMATION & SERVICES	AFRC B&L GI&S	USAF	AFRC	BMA	UNCLASS
Other	AFSCN MISSION SEGMENT	AFSCN MS	USAF	USSF	WMA-Force Support (FS)	UNCLASS

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Logistics & Sustainment	AIRCRAFT HEALTH MONITORING SYSTEM/DATA ANALYSIS AND REDISTRIBUTION TOOL	AHMS/DART	USAF	AFMC	BMA	UNCLASS
Operations	AIRCRAFT INTERTIAL ALIGNMENT SYSTEM	AIAS	Navy	NAVSEA	WMA-Battlespace Awareness (BA)	
Other	ASSESSMENT INFLUENCE MODEL	AIM	USAF	ACC	WMA-Force Application (FA)	SECRET
Logistics & Sustainment	ASSET AND INFORMATION MANAGEMENT	AIM	Navy	NAVAIR	BMA	UNCLASS
Logistics & Sustainment	AUTOMATED INFORMATION MULTIMEDIA MANAGEMENT	AIM2	USAF	HAF	WMA-Logistics (L)	UNCLASS
Other	ADVANCED INTERACTIVE MANAGEMENT TECHNOLOGY CENTER INFORMATION SYSTEM	AIMTCIS	Navy	NAVSEA	BMA	UNCLASS
Operations	AUTOMATIC IDENTIFICATION SYSTEM	AIS	Navy	SPAWAR	WMA-Battlespace Awareness (BA)	SECRET
Logistics & Sustainment	AUTOMATIC IDENTIFICATION TECHNOLOGY	AIT	Navy	NAVSUP	EIEMA-Core Enterprise Services	UNCLASS
Other	AMC KNOWLEDGE MANAGEMENT PORTAL ? CLASSIFIED	AKMP-C	ARMY	AMC - HQAMC - Headquarter, U.S. Army Materiel Command	EIEMA-Core Enterprise Services	SECRET
Other	AMC KNOWLEDGE MANAGEMENT PORTAL ? UNCLASSIFIED	AKMP-U	ARMY	AMC - HQAMC - Headquarter, U.S. Army Materiel Command	EIEMA-Core Enterprise Services	UNCLASS
Logistics & Sustainment	AVIATION AND MISSILE COMMAND (AMCOM) LOGISTICS CENTER WEBDESK	ALC WEBDESK	ARMY	AMC - AMCOM - U.S. Army Aviation and Missile Command	BMA	SBU
Logistics & Sustainment	AVIATION AND MISSILE COMMAND (AMCOM) LOGISTICS CENTER WEBDESK	ALC WEBDESK	ARMY	AMC - AMCOM - U.S. Army Aviation and Missile Command	BMA	SBU
Logistics & Sustainment	NAVAIR AVIATION LOGISTICS ENVIRONMENT	ALE	Navy	NAVAIR	BMA	UNCLASS

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Logistics & Sustainment	AUTOMATED LOGISTICS MANAGEMENT SUPPORT SYSTEM	ALMSS	USAF	AFMC	BMA	UNCLASS
Operations	ARMY LONG-RANGE PERSISTENT SURVEILLANCE (CRN-TIV)	ALPS (CRN-TIV)	ARMY	ASA(ALT) - PEO MS Tactical	WMA-Battlespace Awareness (BA)	Other
Operations	GLOBAL MOBILITY MAPPING AND VISUALIZATION	AMC.maps	USAF	AMC	BMA	UNCLASS
Engineering	AVIATION AND MISSILE COMMAND SAFETY INTERIM HAZARD CLASSIFICATION	AMCOM SIHC	ARMY	AMC - AMCOM - U.S. Army Aviation and Missile Command	BMA	SBU
Operations	AN/SPY-6(V)1 AIR AND MISSILE DEFENSE RADAR	AMDR	Navy	NAVSEA	WMA-Battlespace Awareness (BA)	
Other	AUTOMATED MACHINE LEARNING CAPABILITY	AMLC	DISA	DBC ID	DIMA-Enterprise Information Technology (Aligns with EIEMA)	
Logistics & Sustainment	AIR-TO-SURFACE MUNITIONS DIRECTORATE	AMMO-WEB	USAF	AFMC	BMA	UNCLASS
Operations	AIRBORNE MINE NEUTRALIZATION SYSTEM	AMNS	Navy	NAVSEA	WMA-Force Application (FA)	
Operations	AIRBORNE MINE NEUTRALIZATION SYSTEM SEAFOX AN/ASQ-232A	AMNS SEAFOX	Navy	NAVSEA	WMA-Protection (P)	
Logistics & Sustainment	AIRCRAFT MAINTENANCE PRODUCTION/COMPRESSION REPORT SYSTEM	AMREP	USAF	AFMC	BMA	UNCLASS
Logistics & Sustainment	ARMY MATERIEL SYSTEMS ANALYSIS ACTIVITY - LOGISTICS ANALYSIS DIVISION ORACLE DATA WAREHOUSE	AMSAA - LAD ODW	ARMY	AFC - CCDC - Combat Capabilities Development Command	BMA	
Operations	AN/BQR-22A EC-17	AN/BQR-22A	Navy	NAVSEA	WMA-Battlespace Awareness (BA)	

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Operations	AN/BQS-15	AN/BQS-15	Navy	NAVSEA	WMA-Force Application (FA)	
Operations	AIRCRAFT CONTROL APPROACH CENTRAL	AN/SPN-35C	Navy	NAVAIR	WMA-Battlespace Awareness (BA)	UNCLASS
Operations	INSTRUMENT CARRIER LANDING SYSTEM (ICLS)	AN/SPN-41B ICLS	Navy	NAVAIR	WMA-Battlespace Awareness (BA)	UNCLASS
Operations	PRECISE INTEGRATED NAVIGATION SYSTEM	AN/SSN-2(V) PINS	Navy	NAVSEA	WMA-Battlespace Awareness (BA)	
Operations	ELECTRONIC COUNTERMEASURES RECEIVING SET (AN/WLR-8(V)5)	AN/WLR-8(V)5	Navy	NAVSEA	WMA-Force Application (FA)	
Operations	ELECTRONIC COUNTERMEASURES RECEIVING SET (AN/WLR-8A(V)2)	AN/WLR-8A(V)2	Navy	NAVSEA	WMA-Force Application (FA)	
Operations	AN/WLR-9B(V) SERIES	AN/WLR-9B(V)	Navy	NAVSEA	WMA-Battlespace Awareness (BA)	
Other	AUTOMATED RADIOLOGICAL CONTROLS MANAGEMENT INFORMATION SYSTEM	ARCMIS	Navy	NAVSEA	BMA	UNCLASS
Logistics & Sustainment	AUTOMATED READINESS INFORMATION SYSTEM	ARIS	USAF	AFMC	BMA	UNCLASS
Engineering	ARMY RANGE MAPPER - JMTC/TSAE (EUR)	ARM	ARMY	USAREUR - 7 ATC	WMA-Force Support (FS)	UNCLASS
Logistics & Sustainment	ARMY SUSTAINMENT COMMAND G-2 ADJUDICATION	ASC G-2 ADJUDICATION	ARMY	AMC - ASC - U.S. Army Sustainment Command	BMA	UNCLASS
Engineering	AEROSPACE SYSTEMS DIRECTORATE OPERATIONAL SUPPORT	ASDOS	USAF	AFMC	BMA	UNCLASS
Engineering	AVIATION SYSTEMS INTEGRATION FACILITY (CRN-TIV)	ASIF (CRN-TIV)	ARMY	ASA(ALT) - PEO AVN - Aviation	WMA-Command and Control (C2)	UNCLASS

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Other	ADVANCED SYSTEMS INFORMATION EXCHANGE SERVER	ASIXS	Navy	NAVSEA	BMA	UNCLASS
Other	ALL SITES MODULE	ASM	Navy	NAVSEA	BMA	UNCLASS
Personnel	AIR SOLDIER PERSONAL ELECTRONICS (SIS -T IV)	ASPE (SIS -T IV)	ARMY	ASA(ALT) - PEO Soldier	WMA-Force Application (FA)	SECRET
Operations	ADVANCED TECHNICAL INFORMATION SUPPORT SYSTEM	ATIS	Navy	NAVSEA	BMA	Other
Engineering	AIR FORCE VIRTUAL ANALYSIS CENTER - CLASSIFIED	AVAC	USAF	USSF	WMA-Force Application (FA)	
Security	AEROSOL AND VAPOR CHEMICAL AGENT DETECTOR	AVCAD	ARMY	ASA(ALT) - JPEO-CBD - Joint PEO Chemical and Biological Defense	WMA-Protection (P)	UNCLASS
Engineering	BALLISTIC MISSILE DEFENSE SYSTEM ANALYSIS ELEMENT	BAE	MDA	BC	EIEMA-Computing Infrastructure	SECRET
Operations	MQ-4C TRITON	BAMS UAS	Navy	NAVAIR	WMA-Battlespace Awareness (BA)	SECRET
Engineering	BRASS BOARD HARDWARE IN THE LOOP	BBHWIL	MDA	GM	EIEMA-Computing Infrastructure	SECRET
Other	BLUE CASTLES DATABASE APPLICATION	BC	ARMY	INSCOM - AFSC - Army Field Support Command	EIEMA-Core Enterprise Services	SECRET
Logistics & Sustainment	BOATS INVENTORY MANAGEMENT SYSTEM	BIMS	Navy	NAVSEA	BMA	UNCLASS
Logistics & Sustainment	BARCODE INVENTORY TRACKING SYSTEM	BITS	USAF	AFRC	BMA	
Security	BIOMETRICS OPERATIONS DIRECTORATE CLASSIFIED IDENTITY MISSION SYSTEM	BOD CMS	ARMY	USACID - [None]	EIEMA-Communications	SECRET
Security	BIOMETRICS OPERATIONS DIRECTORATE UNCLASSIFIED IDENTITY MISSION SYSTEM	BOD UIMS	ARMY	USACID - [None]	EIEMA-Communications	UNCLASS

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Intelligence	BLACK RHINO	BR	DTRA	NE-MA	WMA-Protection (P)	TS
Other	CAPS AND LIMS WEBSITE	C&L WEBSITE	Navy	NAVSEA	WMA-Battlespace Awareness (BA)	SECRET
Intelligence	COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS AND INTELLIGENCE SUITE	C4IS	Navy	CNIC	EIEMA-Communications	SECRET
Engineering	CENTRALIZED AVIATION FLIGHT RECORDS SYSTEM 4.0	CAFRS 4.X	ARMY	ASA(ALT) - PEO AVN Tactical	WMA-Force Application (FA)	UNCLASS
Logistics & Sustainment	COMMERCIAL AND GOVERNMENT ENTITY	CAGE	DLA	J62C	BMA	SBU
Logistics & Sustainment	COMBAT SERVICE SUPPORT (CSS) AUTOMATED INFORMATION SYSTEMS INTERFACE	CAISI 2.0	ARMY	ASA(ALT) - PEO C3T	WMA-Logistics (L)	UNCLASS
Logistics & Sustainment	CONTINGENCY AND ADAPTIVE PLANNING SOFTWARE INTEGRATION SYSTEM	CAPIS	DLA	J62P	BMA	SECRET
Operations	COUNTERMEASURE ANTI-TORPEDO	CAT	Navy	NAVSEA	WMA-Protection (P)	
Other	CATAPULT INFORMATION SYSTEM	CATAPULT	DTRA	IT	WMA-Protection (P)	SECRET
Logistics & Sustainment	CAPITAL ASSET TRACKING SYSTEM	CATS	Navy	NAVSEA	BMA	UNCLASS
Engineering	CONSOLIDATED ARCHITECTURE TOOL SUITE	CATS	USTRANSCOM	HQ AMC	WMA-Corporate Management and Support (CMS)	UNCLASS
Operations	CHEMICAL BIOLOGICAL MASS SPECTROMETER II	CBMS II	ARMY	ASA(ALT) - JPEO-CBD - Joint PEO Chemical and Biological Defense	WMA-Protection (P)	UNCLASS
Operations	CHEMICAL BIOLOGICAL RADIOLOGICAL AND NUCLEAR INFORMATION SYSTEM	CBRN-IS	ARMY	ASA(ALT) - JPEO-CBD - Joint PEO Chemical and Biological Defense	WMA-Protection (P)	SECRET

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Operations	CHEMICAL BIOLOGICAL RADIOLOGICAL AND NUCLEAR INFORMATION SYSTEM	CBRN-IS	ARMY	ASA(ALT) - JPEO-CBD - Joint PEO Chemical and Biological Defense	WMA-Protection (P)	Other
Operations	COMBATANT COMMANDERS INTEGRATED COMMAND AND CONTROL SYSTEM SIDES A, B, AND O ENCLAVE	CCIC2S A-B-O	USAF	USSF	WMA-Battlespace Awareness (BA)	
Security	CRYPTOLOGIC CARRY-ON PROGRAM'S GENERIC AREA LIMITATION ENVIRONMENT	CCOP GALE	Navy	SPAWAR	DIMA-Exploitation	SECRET
Data	CLASSIFIED DATA AT REST	CDAR	USAF	ACC	WMA-Force Support (FS)	TS
Logistics & Sustainment	CITS DEPLOYMENT DIAGNOSTIC SYSTEM - WEB SERVER	CDDS-WS	USAF	AFMC	WMA-Logistics (L)	UNCLASS
Operations	COMMUNICATIONS DATA LINK SYSTEM - VIDEO INTERFACE GROUP	CDLS VIG	Navy	SPAWAR	WMA-Battlespace Awareness (BA)	
Engineering	CAPE ENVIRONMENTAL	CE	ARMY	AMC - AMCOM - U.S. Army Aviation and Missile Command	BMA	SBU
Engineering	COMPREHENSIVE ENGINE MANAGEMENT SYSTEM	CEMS (D042)	USAF	AFMC	BMA	UNCLASS
Operations	CLASSIFIED FLEET APPLICATION SUPPORT SYSTEMS	CFASS	Navy	USFFC	EIEMA-Core Enterprise Services	SECRET
Other	CLASSIFIED IRBM MAB SYSTEMS	CIMS	MDA	TC	EIEMA-Computing Infrastructure	SECRET
Other	CONGRESSIONAL INFORMATION MANAGEMENT SYSTEM	CIMS	Navy	CNO-OPNAV	EIEMA-Communications	UNCLASS
Other	CRITICAL MISSION MANAGEMENT TOOL	CMMT	ARMY	AMC - TACOM - U.S. Army Tank-Automotive and Armaments Command	BMA	UNCLASS
Other	CONTINUOUS MONITORING PROGRAM	CMP	Navy	USFFC	BMA	UNCLASS

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Other	CNSL SPEAR	CNSL SPEAR	Navy	USFFC	BMA	UNCLASS
Other	CONTROL-M	CONTROL-M - 17708	DISA	HC33	DIMA-Enterprise Information Technology (Aligns with EIEMA)	SECRET
Operations	CENTER OPERATIONS ON-LINE	COOL	USAF	AFMC	WMA-Force Support (FS)	UNCLASS
Other	CRISIS RESPONSE MANAGEMENT INFORMATION SYSTEM	CRMIS	Navy	CNIC	BMA	UNCLASS
Data	DATA ANALYSIS CONTROL GROUP	DACG	USMC	USMC	WMA-Logistics (L)	Other
Data	DATA ANALYTICS AND INTEGRATION SUPPORT	DAIS	USD(A&S)	OASD (EI&E)	BMA	UNCLASS
Data	DATA ANALYSIS SYSTEM	DAS	Navy	COMPACFLT	WMA-Battlespace Awareness (BA)	SECRET
Data	DATA ANALYSIS SYSTEM	DAS	Navy	COMPACFLT	WMA-Battlespace Awareness (BA)	SECRET
Other	DIRECT CLARITY-S	DC-S	DTRA	PP-SC	WMA-Protection (P)	SECRET
Other	DIRECT CLARITY-U	DC-U	DTRA	PP-SC (SCC)	WMA-Protection (P)	UNCLASS
Operations	DDG 1000 CLASSIFIED INTEGRATED DATA ENVIRONMENT	DDG 1000 CLASSIFIED IDE	Navy	NAVSEA	EIEMA-Core Enterprise Services	SECRET
Operations	DDG 1000 INTEGRATED DATA ENVIRONMENT	DDG 1000 IDE	Navy	NAVSEA	EIEMA-Core Enterprise Services	UNCLASS
Operations	DDG 1000 TOTAL SHIP COMPUTING ENVIRONMENT	DDG 1000 TSCE	Navy	NAVSEA	WMA-Protection (P)	SECRET
Operations	DDG MODERNIZATION INTEGRATED BRIDGE NAVIGATION SYSTEM	DDG IBNS	Navy	NAVSEA	WMA-Force Application (FA)	SECRET
Operations	DDG 51 INTEGRATED BRIDGE SYSTEM	DDG51 IBS	Navy	NAVSEA	WMA-Net Centric (NC)	Other

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Logistics & Sustainment	DECISION KNOWLEDGE PROGRAMMING FOR LOGISTICS ANALYSIS AND TECHNICAL EVALUATION	DECKPLATE	Navy	NAVAIR	BMA	UNCLASS
Engineering	DEVCOM-AVMC-RUBIX	DEVCOM-AVMC-RUBIX	ARMY	AFC - CCDC - Combat Capabilities Development Command	BMA	UNCLASS
Data	DATA HOUSING AND REPORTS TOOL, SUITE OF TOOLS	DHART	ARMY	Provost Marshal - [None]	BMA	UNCLASS
Intelligence	KZO	DIA-KZO	DIA	ADI	BMA	TS
Security	DISCSWEB	DISCSWEB	DSCA	DISCS	BMA	UNCLASS
Logistics & Sustainment	DISPOSITION INTEGRATION WEB	DIW	DLA	J62C	BMA	UNCLASS
Other	DECISION LENS WEB	DLW	Navy	CNIC	BMA	UNCLASS
Logistics & Sustainment	DYNAMIC MISSION REPLANNING	DMR	USTRANSCOM	HQ AMC	WMA-Logistics (L)	SBU
Other	DEPARTMENT OF THE NAVY INTEGRATED BOARDING SYSTEM - ATLAS	DONIBS-ATLAS	DON		BMA	UNCLASS
Engineering	DEVOPS RELEASE MANAGEMENT SYSTEM	DORMS	USD(A&S)	DBO	EIEMA-Computing Infrastructure	UNCLASS
Operations	DISTRIBUTED SPACE COMMAND AND CONTROL - DAHLGREN MISSION PROCESSING SYSTEM	DSC2-D MPS	USAF	USSF	WMA-Battlespace Awareness (BA)	SECRET
Logistics & Sustainment	DEVSECOPS-AZURE	DSOA	DLA		EIEMA-Computing Infrastructure	UNCLASS
Operations	DECISION SUPPORT SYSTEMS - CLASSIFIED	DSS-C	USSTRATCOM		WMA-Command and Control (C2)	TS
Engineering	DTRA MISSION ASSESSMENT AND ANALYSIS SYSTEM	DTRA MAAS	DTRA	IT	BMA	SECRET

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Operations	ENTERPRISE COMMAND AND CONTROL - KIRTLAND AFB	EC2-K	USAF	USSF	WMA-Command and Control (C2)	SECRET
Security	ELECTRONIC COMBAT INTERNATIONAL SECURITY ASSISTANCE PROGRAM	ECISAP-CSS	DSCA	IM&T	WMA-Net Centric (NC)	
Data	ENVIRONMENTAL DATA ENTERPRISE - CLASSIFIED	EDE-C	DTRA	RD	WMA-Protection (P)	SECRET
Data	ENVIRONMENTAL DATA ENTERPRISE - UNCLASSIFIED	EDE-U	DTRA	RD	WMA-Protection (P)	SBU
Other	ENTERPRISE HUB	E-HUB	USMC		DIMA-Enterprise Information Technology (Aligns with EIEMA)	SECRET
Other	ENVIRONMENTAL INFORMATION MANAGEMENT SYSTEM	EIMS	Navy	USFFC	BMA	UNCLASS
Operations	EVENTS LOGBOOK (JS)	ELB	JOINT STAFF	J35	WMA-Command and Control (C2)	SECRET
Other	ENTERPRISE MANAGEMENT INFORMATION SYSTEM	EMIS	USAF	AFMC	BMA	UNCLASS
Operations	ENHANCED MONITORING SYSTEM (EMS)	EMS	USAF	USSF	WMA-Battlespace Awareness (BA)	SECRET
Other	ENCHILADA	ENCHILADA	Navy	NAVSEA	BMA	UNCLASS
Logistics & Sustainment	ELECTRONIC STORAGE AND RETRIEVAL SYSTEM	ESRS	Navy	NAVAIR	BMA	UNCLASS
Intelligence	AF.01.LACKLAND.ACC.EWOPS	EWOPS	USAF	ACC	WMA-Battlespace Awareness (BA)	TS
Logistics & Sustainment	EXPEDITIONARY MANAGEMENT INFORMATION SYSTEM	EXMIS	Navy	NAVFAC	BMA	UNCLASS

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Security	FORENSICS DOMINANCE SYSTEM - MARINE COPRS	FDS-MC	USMC		WMA-Battlespace Awareness (BA)	
Operations	FORCE LEVEL INTEGRATION	FLINT	Navy		BMA	SECRET
Logistics & Sustainment	FEDERAL LOGISTICS INFORMATION SYSTEM	FLIS	DLA	J62H	BMA	UNCLASS
Engineering	FORGE-SECRET	FORGE-S	ARMY	AFC - FCC - Future and Concepts Center	WMA-Force Application (FA)	SECRET
Operations	FORWARD OBSERVER SYSTEM	FOS	ARMY	ASA(ALT) - PEO C3T	WMA-Force Application (FA)	SECRET
Operations	FORWARD OBSERVER SYSTEMS V11	FOS V11	ARMY	ASA(ALT) - PEO C3T	WMA-Force Application (FA)	SECRET
Operations	FORCE SURVIVABILITY, ANALYSIS, AND MANAGEMENT	FSAM	USSTRATCOM		WMA-Command and Control (C2)	TS
Other	HQMC G10 ANALYSIS DATA ENVIRONMENT	GADE	USMC		EIEMA-Computing Infrastructure	
Engineering	GLOBAL LOW	Global Low	MDA	BC	EIEMA-Communications	SECRET
Security	GLOBALNET	GLOBALNET	DSCA	CMO	BMA	UNCLASS
Operations	GRANITE LOOK TRACKER	GLT	ARMY	HQDA G3 - OD	BMA	SECRET
Operations	GLOBAL MANAGEMENT CENTER	GMC	DISA	OPC FC	DIMA-Enterprise Management Support (Aligns with BMA)	SECRET
Engineering	GEODETIC SURVEY SET	GSS	USMC	USMC	DIMA-Collection	UNCLASS
Operations	GEOSTATISTICAL TEMPORAL-SPATIAL (GTS) LONG-TERM MONITORING OPTIMIZATION	GTS	USAF	AFMC	BMA	UNCLASS
Engineering	HOLISTIC, ADAPTIVE, MULTI-MISSION EVENT RESOURCE SYSTEM	HAMMERS	MDA	DT	EIEMA-Communications	SECRET

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Operations	JOINT COMMAND CENTER - MODERNIZATION	I CORPS JCC	ARMY	FORSCOM - I Corps	WMA-Command and Control (C2)	SECRET
Operations	INTEGRATED AIR & MISSILE DEFENSE	IAMD	ARMY	ASA(ALT) - PEO MS Tactical	WMA-Protection (P)	SECRET
Operations	INTERMEDIARY APPLICATION	IAPP	Navy	SPAWAR	WMA-Command and Control (C2)	SECRET
Other	INTEGRATED COMMON PROCESSOR	ICP	Navy	NAVSEA	WMA-Battlespace Awareness (BA)	SECRET
Data	INTEGRATED DATABASE SYSTEM SUPPORT CLASSIFIED	IDSS-C	USAF	USSF	WMA-Command and Control (C2)	SECRET
Data	INTEGRATED DATABASE SYSTEM SUPPORT UNCLASS	IDSS-U	USAF	USSF	WMA-Command and Control (C2)	UNCLASS
Logistics & Sustainment	INTEGRATED INFORMATION MANAGEMENT SYSTEM	IIMS	USAF	AFMC	BMA	SBU
Logistics & Sustainment	INTEGRATED INFORMATION TOOL	IIT	USAF	AFMC	BMA	UNCLASS
Engineering	INSTRUMENTATION LOADING, INTEGRATION, ANALYSIS, AND DECOMMUTATION SYSTEM	ILIAD	USAF	AFMC	WMA-Force Application (FA)	UNCLASS
Logistics & Sustainment	INTEGRATED MULTI-MODAL OPERATIONS	IMMO	USTRANSCOM	USTRANSCOM	WMA-Command and Control (C2)	UNCLASS
Data	INTEGRATED DATABASE	Integrated Database	USAF	AFMC	BMA	UNCLASS
Intelligence	INTEL 12	INTEL 12	ARMY	INSCOM - HQ INSCOM - Headquarters Intelligence and Security Command	DIMA-Analysis and Production	SECRET
Intelligence	INTEL 13	INTEL 13	ARMY	INSCOM - HQ INSCOM - Headquarters Intelligence and Security Command	DIMA-Collection	SBU

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Intelligence	INTEL 20	INTEL 20	ARMY	INSCOM - GISA-Europe - Ground Intelligence Support Activity - Europe	DIMA-Enterprise Information Technology (Aligns with EIEMA)	SBU
Intelligence	INTEL 21	INTEL 21	ARMY	INSCOM - GISA-Europe - Ground Intelligence Support Activity - Europe	DIMA-Enterprise Information Technology (Aligns with EIEMA)	SECRET
Security	IDENTITY RESOLUTION EXPLOITATION MANAGEMENT SERVICES	IREMS-C	ARMY	AFC - CCDC - Combat Capabilities Development Command	WMA-Battlespace Awareness (BA)	SECRET
Other	INFERENTIAL RETRIEVAL INDEXING SYSTEM	IRIS	USAF	HAF	BMA	SBU
Intelligence	INTERNAL RESOURCES MANAGEMENT APPLICATION - INTELLIGENCE	IRMA-I	USD(I)	CHIEF OF STAFF	BMA	UNCLASS
Intelligence	JOINT ANALYTIC REAL-TIME VIRTUAL INFORMATION SHARING SYSTEM	JARVISS	ARMY	Provost Marshal - [None]	BMA	SBU
Logistics & Sustainment	JOINT EXPLOSIVE ORDNANCE DISPOSAL DECISION SUPPORT SYSTEM PORTAL CLASSIFIED	JEOD DSS PORTAL S	Navy	NAVSEA	WMA-Force Support (FS)	SECRET
Logistics & Sustainment	JWICS MISSION ASSURANCE NETWORK	JMAN	USSTRATCOM		EIEMA-Computing Infrastructure	
Operations	JOINT MANAGEMENT OPERATIONS SUBSYSTEM - CLASSIFIED (JMOSC)	JMOSC	ARMY	ASA(ALT) - PEO EIS PM DCATS - Program Manager, Defense Communications and Army Transmissions Systems	WMA-Command and Control (C2)	SECRET
Operations	JOINT MANAGEMENT OPERATIONS SUBSYSTEM UNCLASSIFIED	JMOSU	ARMY	ASA(ALT) - PEO EIS PM DCATS - Program Manager, Defense Communications and Army Transmissions Systems	WMA-Command and Control (C2)	UNCLASS

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Engineering	JOINT MULTI-NATIONAL READINESS CENTER - INSTRUMENTATION SYSTEM	JMRC-IS	ARMY	ASA(ALT) - PEO STRI - PM ST	WMA-Force Support (FS)	SBU
Requirements	KNOWLEDGE MANAGEMENT AND DECISION SUPPORT TOOL	KM/DS	JOINT STAFF	J8	WMA-Corporate Management and Support (CMS)	SECRET
Operations	KEYMAKER	KM-S	ARMY	SMDC - [None]	WMA-Command and Control (C2)	SECRET
Operations	LAUNCH AREA PHOTOGRAPHIC SYSTEM	LAPS	Navy	COMPACFLT	WMA-Command and Control (C2)	
Operations	LINK MONITORING AND MANAGEMENT TOOL	LMMT	Navy	SPAWAR	WMA-Command and Control (C2)	SECRET
Logistics & Sustainment	MARINE AMMUNITION KNOWLEDGE ENTERPRISE	MAKE	USMC	USMC	BMA	UNCLASS
Intelligence	AFMC COMBAT SUPPORT LOCATION INTELLIGENCE	Maps.AFMC	USAF	AFMC	BMA	UNCLASS
Logistics & Sustainment	MAXIMO ENTERPRISE	MAXIMO	Navy	NAVFAC	BMA	UNCLASS
Security	MARSHALL CENTER NET	MC NET	DSCA	GCMC	BMA	UNCLASS
Intelligence	MARINE CORPS COMMON ALL SOURCE SERVER APPLICATIONS	MCCASSA	USMC		DIMA-Analysis and Production	SECRET
Data	ENTERPRISE PRODUCT DATA MANAGEMENT	MCI-AFC-DEVCOM-EPDM	ARMY	AFC - CCDC - Combat Capabilities Development Command	BMA	UNCLASS
Other	MCITC MCICOM PORTAL	MCITC MCICOM PORTAL	USMC	USMC	BMA	UNCLASS
Data	MOBILE DATA ARCHIVE AND RETRIEVAL(898)	MDAR	ARMY	ASA(ALT) - PEO AVN Tactical	WMA-Battlespace Awareness (BA)	SECRET
Data	METROLOGY DATA SYSTEMS	MDS	Navy	NAVSEA	BMA	UNCLASS

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Intelligence	MARINE EXPEDITIONARY FORCE INTELLIGENCE ANALYSIS SYSTEM	MEF IAS	USMC	USMC	DIMA-Analysis and Production	SECRET
Other	MCEN EVENT MANAGEMENT SYSTEM	MEMS	USMC	USMC	EIEMA-Core Enterprise Services	SECRET
Engineering	METROLOGY APPLICATION SOFTWARE SUITE	Metweb	USAF	AFMC	BMA	UNCLASS
Operations	MARITIME OPERATIONS CENTER (MOC) IN THE MIDDLE	MITM	Navy	SPAWAR	WMA-Command and Control (C2)	SECRET
Operations	MISSION OPERATIONS CENTER/MISSION SUPPORT CENTER	MOC/MSC	MDA	SN	WMA-Force Support (FS)	SECRET
Data	MANAGEMENT SUPPORT AND DATA ANALYSIS (MSADA)	MSADA	Navy	NAVSEA	BMA	UNCLASS
Other	MINE AND UNDERSEA WARFARE INFORMATION DESK	MUW INFODESK	Navy	NAVSEA	EIEMA-Core Enterprise Services	UNCLASS
Engineering	NUCLEAR CHEMICAL BIOLOGICAL RADIOLOGICAL AND HIGH EXPLOSIVES ANALYSIS TOOLSET	NATS	DTRA	RD	WMA-Net Centric (NC)	UNCLASS
Other	NEWPORTAL	NEWPORTAL	Navy	NAVSEA	EIEMA-Core Enterprise Services	UNCLASS
Other	NEWPORTAL	NEWPORTAL	Navy	NAVSEA	EIEMA-Core Enterprise Services	UNCLASS
Other	NEWTON	NEWTON	DISA	OC NLCC	DIMA-Enterprise Information Technology (Aligns with EIEMA)	UNCLASS
Engineering	NORTH ISLAND CMPRO SYSTEM	NICMPRO	Navy	NAVAIR	BMA	UNCLASS
Other	PIT-SREL-NMARS-CLOUDONE	NMARS	USAF	ACC	WMA-Battlespace Awareness (BA)	

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Logistics & Sustainment	NORMALIZED DATABASE	NORM	Navy	NAVFAC	BMA	UNCLASS
Engineering	NOSIS	NOT AN ACRONYM	Navy	NAVSEA	WMA-Force Support (FS)	SECRET
Operations	ORBITAL ANALYSIS SUBSYSTEM	OAS	USAF	USSF	WMA-Command and Control (C2)	
Other	OPTICAL DIGITAL IMAGING-RECORDS MANAGEMENT SYSTEM	ODI-RMS	USMC	USMC	BMA	UNCLASS
Operations	OPERATIONAL ENVIRONMENTAL MANAGEMENT	OEM	Navy	NAVAIR	BMA	UNCLASS
Engineering	OVERLORD GROUND STATION SYSTEM	OGS	USAF	AETC	WMA-Command and Control (C2)	SECRET
Operations	OPERATIONAL INFORMATION MANAGEMENT SYSTEM	OIMS	DTRA	IT	WMA-Net Centric (NC)	Other
Logistics & Sustainment	O & M ENTERPRISE SYSTEM	OMES	USAF	AFMC	BMA	UNCLASS
Security	OSI RECORDS, INVESTIGATIONS, AND OPERATIONS NETWORK	ORION	USAF	HAF	BMA	UNCLASS
Operations	OPERATIONALLY RESPONSIVE SPACE - FIVE SENSORSAT	ORS-5 SensorSat	USAF	USSF	WMA-Command and Control (C2)	SECRET
Security	GROUND-BASED MIDCOURSE DEFENSE OPERATIONAL SECURITY BASELINE	OSB	MDA	GM	WMA-Protection (P)	SECRET
Operations	OPERATIONAL SUPPORT SYSTEM - SYSTEM SUPPORT ENVIRONMENT	OSS-SSE	DISA	DBC ID	DIMA-Enterprise Information Technology (Aligns with EIEMA)	SECRET
Operations	OPERATIONAL TOOLS ENHANCEMENT	OTE	USAF	USSF	WMA-Force Support (FS)	SECRET

Subject Area	Name	Acronym	Component	Sub Component	Mission Area-Domain	Network Classification
Personnel	PROCESSING AND DISPLAY SYSTEM - MIGRATION FORWARD USER	PDS-M FU	USAF	USSF	WMA-Command and Control (C2)	SECRET
Security	PERCEPTOR	PERCEPTOR	DISA	DBC ID	EIEMA-Information Assurance	SBU
Logistics & Sustainment	PRODUCTION INFORMATION DATABASE SYSTEM	PIDS II	USAF	AFMC	EIEMA-Core Enterprise Services	UNCLASS
Intelligence	PROPHET ES & CONTROL	PROPHET ES-C	ARMY	ASA(ALT) - PEO IEW&S PM EW&S - Electronic Warfare & Cyber	WMA-Battlespace Awareness (BA)	TS
Operations	RADESNET-SECURE	RADESNet-S	USAF	ACC	WMA-Protection (P)	
Engineering	RANGE DATA PRODUCTS GROUP	RDPG	Navy	COMPACFLT	EIEMA-Computing Infrastructure	SECRET
Intelligence	REAL-TIME EXTRACTION AND ANALYSIS PROCESSOR	REAP	Navy	NAVSEA	WMA-Command and Control (C2)	SECRET
Intelligence	CLUSTER REVERB	REVERB	Navy	ONI	DIMA-Analysis and Production	SECRET
Intelligence	AF.22.LACKLAND.ACC.SDEV	SDEV	USAF	ACC	WMA-Battlespace Awareness (BA)	SECRET
Intelligence	AF.08.LACKLAND.ACC.SPROD	SPROD	USAF	ACC	WMA-Battlespace Awareness (BA)	SECRET
Intelligence	AF.08.LACKLAND.ACC.STORMCLOUD	STORMCLOUD	USAF	ACC	WMA-Battlespace Awareness (BA)	SECRET
Operations	G-2 OPERATIONAL ENVIRONMENT MISSION SYSTEM	TRADOC G2 OE MS	ARMY	TRADOC - HQ - TRADOC HQ	WMA-Battlespace Awareness (BA)	UNCLASS

Appendix F. Dependency Analysis

Introduction

On August 25, 2022, the DoD released the CHMR-AP) The plan, directed by the Secretary of Defense, creates new institutions and processes that will improve strategic outcomes, optimize military operations, and strengthen DoD's ability to mitigate CH during operations through a reinforcing framework.

The action plan is made up of 11 OBJs, each with phased actions to document expected activities. Many of the OBJ have interdependencies with others; instances where guidance or data generated from one OBJ will be used by another to inform its own activities. OBJ 6 of the CHMR-AP tasks SECARMY with the development of standardized CH operational reporting and data management processes to improve how DoD collects, shares, and learns from data related to CH. This task will be informed by activities and data that other OBJs develop (i.e., inputs) and will also provide standards and a platform that the other OBJs will need to leverage (i.e., outputs).

Analytic Approach

This memorandum analyzes the interdependencies that OBJ 6 has amongst the other 10 OBJs, identifying whether the activity provides an input to OBJ 6 or whether OBJ 6 should provide an output for the activity. These activities are further characterized by the type of activity taking place:

- Guidance: Policies, strategies, or lessons learned that will influence OBJ 6 or that OBJ 6 needs to provide for another action.
 - Example Input: Develop and issue a Chairman's Instruction on CHMR to further provide guidance on CHMR efforts across the joint force. [Action 3.d]
 - Example Output: Submit legislative proposals to DoD Legislative Programs for consideration in the NDAA for FY24 to support necessary authorities in CHMR OBJs. [Action 8.b]
- Platform: Anything that effects the DMP. Inputs would provide data feeds or requirements while outputs are any actions that either needs the data platform to be successful or uses data from it.
 - Example Input: Develop federated and reach back support throughout the Defense Intelligence Enterprise to provide CHMR-related information and

expertise, including robust characterizations of the civilian environment in operational areas, to inform joint targeting. [Action 4.c]

- Example Output: Establishing shared information capabilities and processes that support understanding of the civilian environment, including intelligence sharing, as appropriate. [Action 10.c.iii]
- Resourcing: Actions that influence resources relevant to OBJ 6, including training, workforce, or budgetary concerns.
 - Example Input: Develop the career tracks and skill identifiers to support personnel requirements of the joint force to incorporate understanding, visualization, and description of the civilian environment, including during joint targeting. [Action 4.h]
 - Example Output: Submit an issue paper for the FY24–FY28 Program and Budget Review for resources across the CHMR enterprise. [Action 2.f]

Summary of Analysis

OBJ 6 has interdependencies with 133 of 170 CHMR-AP actions, as shown in Table F-1. This memorandum analyzes these interdependencies by their relationship to OBJ 6, key coordinators, and temporal phases. Of all OBJ 6 interdependencies, 88 are inputs and 51 are outputs. OBJ 7, which guides the establishment of Department-wide CHMR procedures, and OBJ 9, which integrates CHMR into security cooperation and multinational operations, have the highest number of OBJ 6 inputs and outputs. Of the 37 actions identified as self-contained (i.e., neither inputs nor outputs to OBJ 6), most are concentrated in OBJ 8. These OBJ 8 actions drive CH response policy change, including guidance for the use of sympathy and condolence payments.

Table F-1. Interdependency Counts by Objective and Dependency

OBJ	Dependent	Self-Contained	Total
OBJ 1: Establish CHMR Steering Committee	2	2	4
OBJ 2: Establish Civilian Protection Center of Excellence	8	3	11
OBJ 3: Institutionalize CHMR Guidance	16	1	17
OBJ 4: Integrate CHMR into Joint Targeting	13	1	14
OBJ 5: Improve Positive Identification	8	3	11
OBJ 7: Establish Department-Wide CH Procedures	27	9	36
OBJ 8: Refresh DoD CH Guidance	11	12	23
OBJ 9: Integrate CHMR into Security Cooperation	20	4	24

OBJ	Dependent	Self-Contained	Total
OBJ 10: Refresh Multinational CH Guidance	18	0	18
OBJ 11: Resource CHMR	10	2	12
Total	133	37	170

OBJ 6 Inputs

Among these 133 interdependencies, 88 are inputs to OBJ 6. These actions inform or impact the way in which OBJ 6 is carried out. Table F-2 depicts the distribution of inputs across OBJs. Inputs are concentrated in OBJ 7, which mandates the establishment of DoD-wide CH assessment and investigation procedures. OBJ 9, which integrates CHMR principles and processes into security cooperation efforts and multinational operations, also provides a large number of inputs to OBJ 6. OBJ 3 directs incorporation of CHMR guidance into strategy, doctrine, plans, and exercises, and provides the third largest number of inputs.

Table F-2. Inputs by Objective and Type

OBJ	Guidance	Platform	Resourcing	Total
OBJ 1	1	0	0	1
OBJ 2	1	1	2	4
OBJ 3	10	2	0	12
OBJ 4	1	8	1	10
OBJ 5	4	1	0	5
OBJ 7	8	8	1	17
OBJ 8	6	3	0	9
OBJ 9	9	7	0	16
OBJ 10	7	3	0	10
OBJ 11	2	0	2	4
Total	49	33	6	88

These inputs were further categorized by type. A majority of inputs are guidance, with the documentation requirements in OBJ 3 again being major contributors. Within the

platform inputs, OBJs 4 and 7 are the major contributors. OBJ 4 discusses data elements and processes that feed the DMP laid out in OBJ 6—as does OBJ 7, which requires CCMDs and the Joint Staff to implement new reporting requirements and CHMR process updates. Figure F-1 shows how inputs are distributed across coordinators (such as the CCMDs and entities within DoD). The CCMDs and Joint Staff are the main input coordinators, though CCMDs have more platform inputs than the Joint Staff.

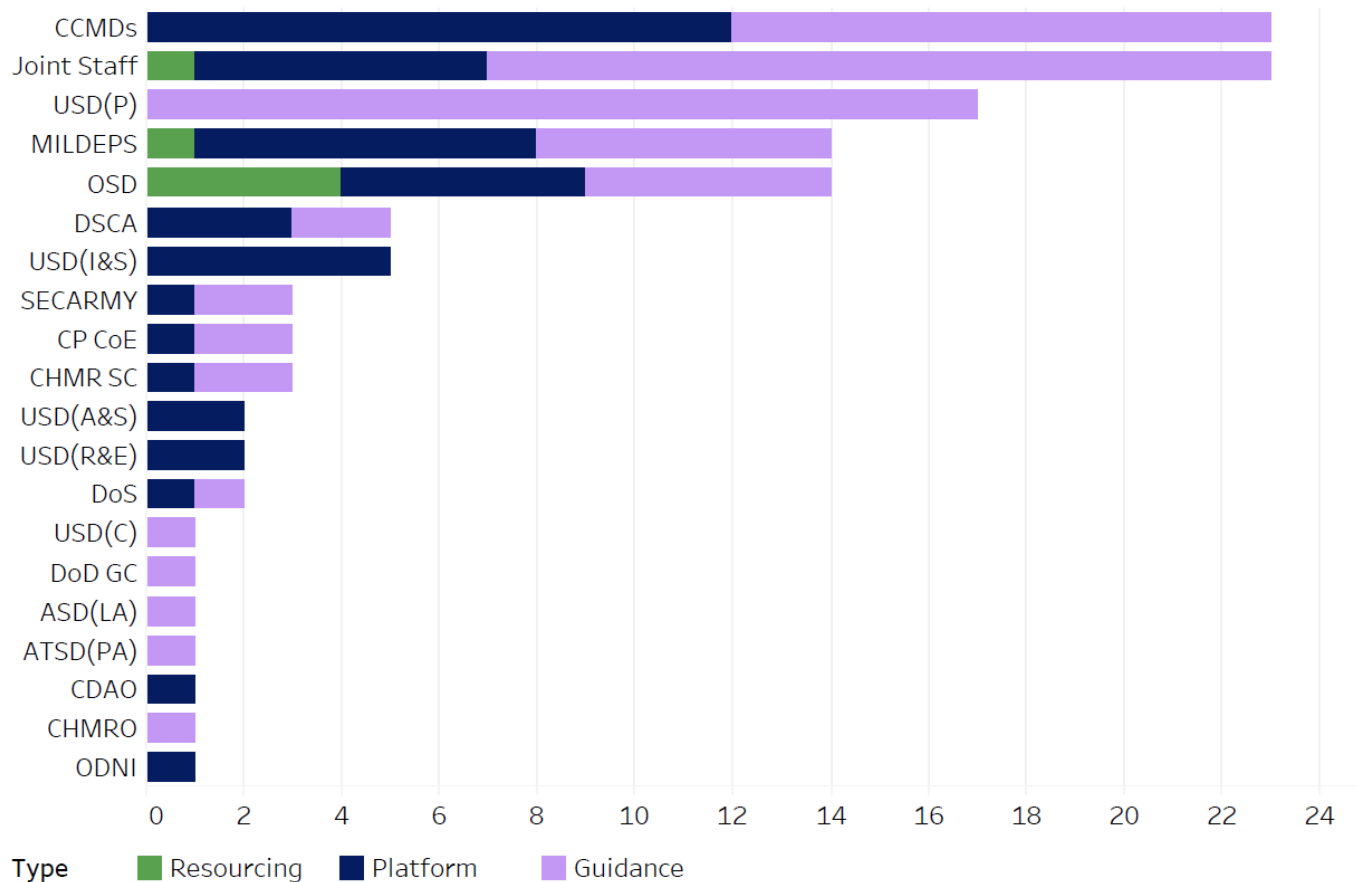


Figure F-1. Input Coordinators by Action Count

CHMR-AP actions are sequenced by phases, beginning with Phase 0 in FY22, Phase 1 in FY23, Phase 2 in FY24, and Phase 3 in FY25. Some actions may be initiated sooner than prescribed, and others may persist across phases. Table F-3 depicts the distribution of inputs across OBJs and phases. Figure F-2 aggregates across OBJs to show the distribution of inputs across phases. A majority of inputs are concentrated in Phase 0 or Phase 1, meaning they are scheduled to occur earlier in the CHMR-AP implementation timeline. DMP deployment is sequenced for Phase 3, meaning the platform may not have the opportunity to incorporate any OBJ 6 inputs also sequenced in Phase 3.

Table F-3. Inputs by Objective and Phase

OBJ	Phase 0	Phase 1	Phase 2	Phase 3	Total
OBJ 1	1	0	0	0	1
OBJ 2	2	0	1	1	4
OBJ 3	2	8	2	0	12
OBJ 4	1	9	0	0	10
OBJ 5	0	5	0	0	5
OBJ 7	10	6	0	1	17
OBJ 8	2	6	0	1	9
OBJ 9	2	5	8	1	16
OBJ 10	1	6	2	1	10
OBJ 11	2		1	1	4
Total	23	45	14	6	88

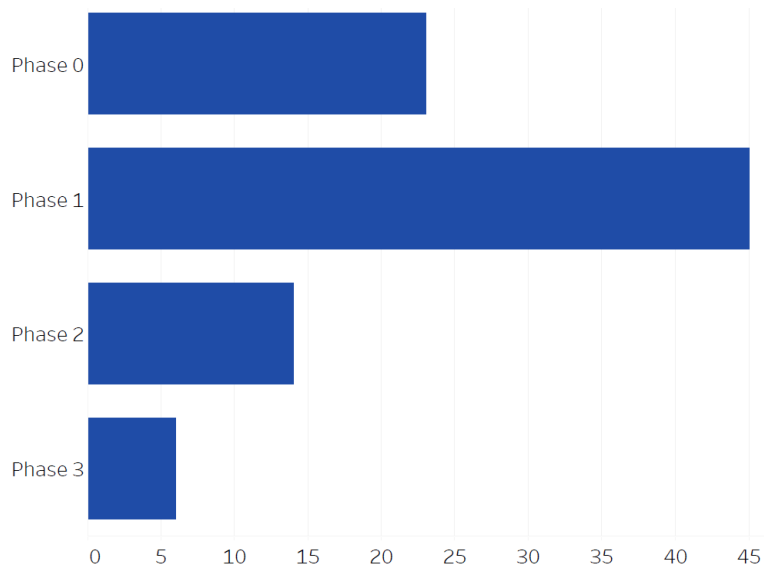


Figure F-2. Input Distribution by Phase

OBJ 6 Outputs

Turning to outputs, 51 interdependencies are outputs relative to OBJ 6, meaning OBJ 6 impacts their completion. A majority of outputs are concentrated in OBJ 7, which

establishes DoD-wide CHMR procedures, and OBJ 9, which integrates CHMR into ally and partner efforts. These same two OBJs also provided the largest number of OBJ 6 inputs. The continued prevalence of OBJ 7 and OBJ 9 across both inputs and outputs indicates they have a substantial impact on OBJ 6 activities. Table F-4 depicts outputs by objective and type.

Table F-4. Outputs by Objective and Type²⁷

OBJ	Guidance	Platform	Resourcing	Total
OBJ 1	1	0	0	1
OBJ 2	1	1	3	5
OBJ 3	3	2	0	5
OBJ 4	1	3	0	4
OBJ 5	3	0	0	3
OBJ 7	2	9	0	11
OBJ 8	1	2	0	3
OBJ 9	3	2	0	5
OBJ 10	3	6	0	9
OBJ 11	1	0	6	7
Total	19	25	9	53

Assessing outputs by type indicates that a majority of OBJ 6 outputs impact the DMP—meaning these actions either rely on the DMP or data it produces. The 19 outputs coded as guidance indicate where OBJ 6 needs to provide documentation (e.g., policies, strategies, or lessons learned) to inform the actions of other OBJs.

Looking across entities that OBJ 6 outputs inform, the CCMDs again are the most prevalent. This is consistent with requirements that CCMDs utilize the DMP. The prevalence of the Joint Staff and USD(P) are also consistent with CHMR actions requiring these entities to integrate the DMP into guidance and training documentation, among other responsibilities. Figure F-3 shows the full distribution of OBJ 6 outputs across coordinators by output type.

²⁷ Some actions are categorized in more than one type. This accounts for tables that report more than 51 outputs.

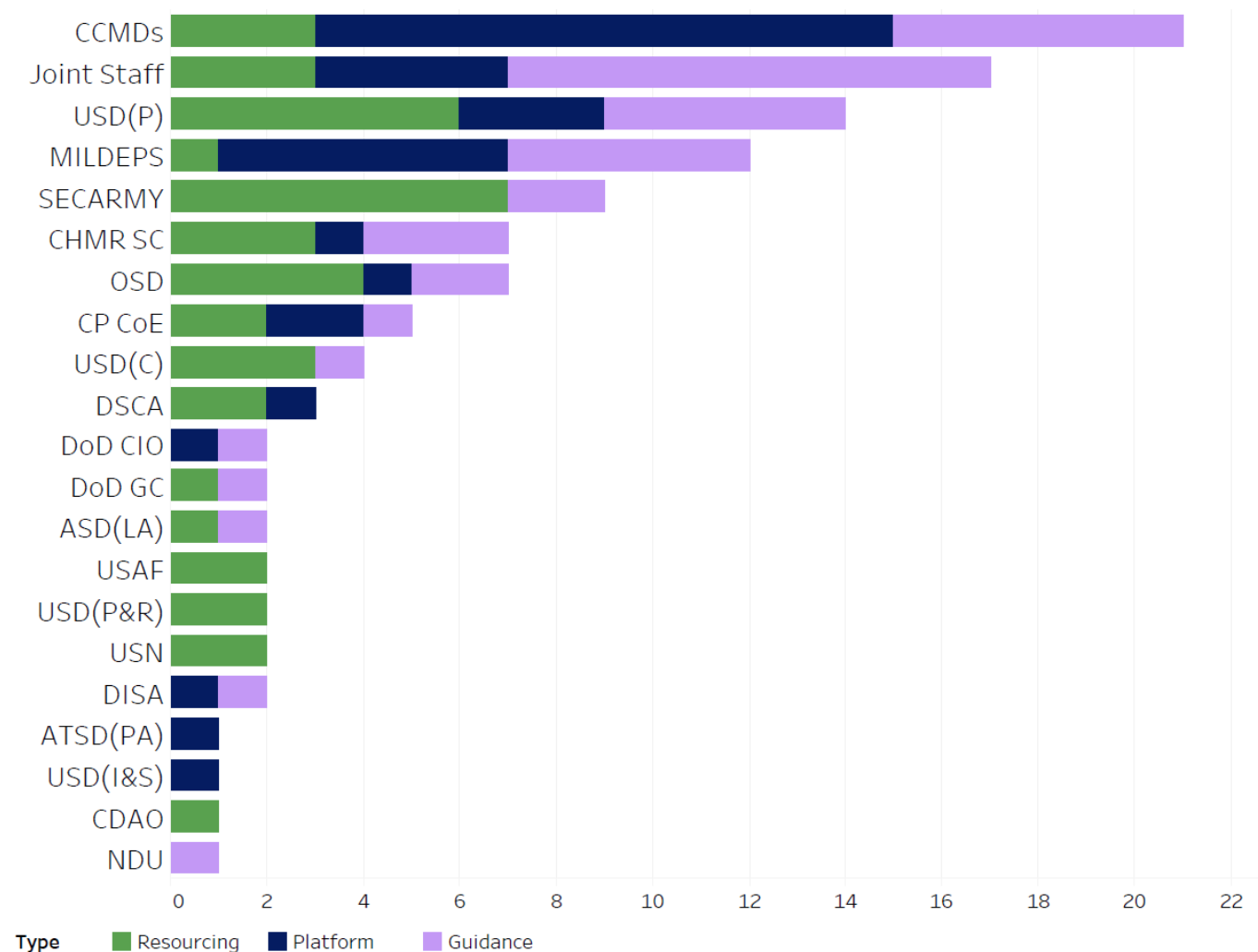


Figure F-3. Output Coordinators by Action Count

Most outputs are sequenced in Phase 0 or Phase 1, indicating OBJ 6 impacts are concentrated early on in CHMR-AP implementation, as planned. Though inputs are also concentrated in Phase 0 or Phase 1, a comparatively smaller ratio of outputs appear in Phase 3. This indicates that OBJ 6 continues to be impacted by late-phase inputs even as most of its impacts have already been dealt. Table F-5 depicts the distribution of outputs across OBJs and phases, and Figure F-4 aggregates outputs across objectives to show the distribution of inputs across phases.

Table F-5. Outputs by Objective and Phase

OBJ	Phase 0	Phase 1	Phase 2	Phase 3	Total
OBJ 1	0	1	0	0	1
OBJ 2	2	2	0	1	5

OBJ 3	0	1	4	0	5
OBJ 4	1	2	0	0	3
OBJ 5	0	3	0	0	3
OBJ 7	6	2	2	1	11
OBJ 8	2	1	0	0	3
OBJ 9	3	2	0	0	5
OBJ 10	0	7	1	0	8
OBJ 11	2	3	2	0	7
Total	16	24	9	2	51

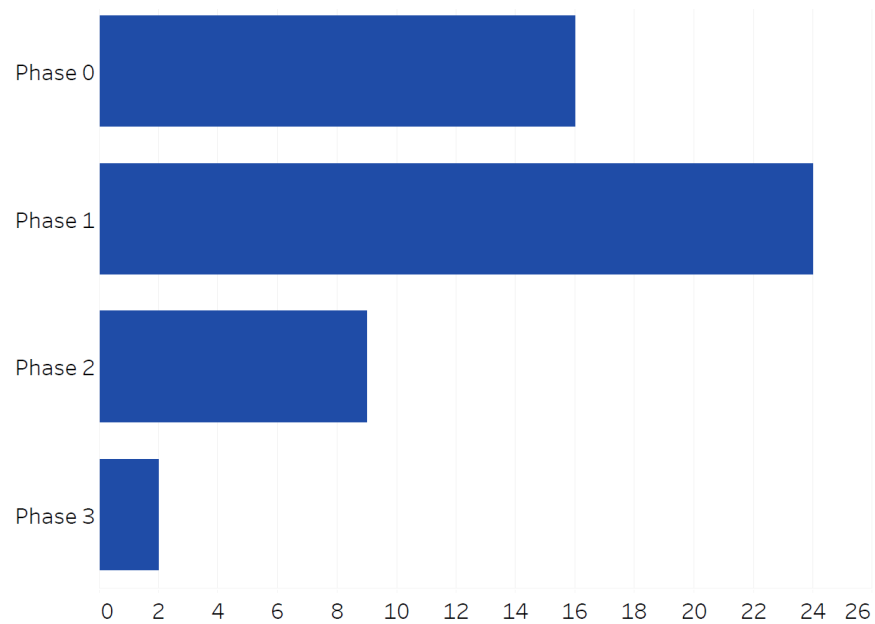


Figure F-4. Output Distribution by Phase

Appendix G. CHMR OBJ 6 Technical Exchange Meeting Proceedings²⁸

Subject: Proceedings – Civilian Harm Mitigation and Response Action Plan (CHMR-AP) Objective 6 Data Management Platform (DMP) Technical Exchange Meeting (TEM)

Date: June 15, 2023

Background and Objectives

On June 15, 2023, SES Adam Nucci and COL Steve Gandia of Headquarters, Department of the Army (HQDA), G3/5/7 held a Technical Exchange Meeting (TEM) at the Institute for Defense Analyses (IDA) to baseline understanding and develop information requirements for the CHMR-AP DMP. Attendees from 21 government organizations, including three military departments and four combatant commands (CCMDs), discussed DMP user stories, identifying the information requirements and data sources for the DMP. (For a full list of participants, see [TEM Participants](#).)

The DMP, defined in Objective 6 of the CHMR-AP, is a critical engine that will provide analytics and reporting about civilian harm (CH) to Civilian Harm Resource Officers (CHMROs), facilitate timely government responses, and inform CH-related training. Figure 1 illustrates the role the DMP might play in the form of an inputs, constraints, outputs, and mechanisms (ICOM) model.

There were four TEM objectives:

- Baseline the understanding of the Objective 6 effort across the relevant organizations.
- Establish 6f as a key milestone in DMP development.
- Build a set of prioritized user stories.
- Collect information requirements and related systems.

This memorandum summarizes the major themes, friction points, information requirements, and action items discussed at the event.

²⁸ This memorandum is reprinted here in its original format.

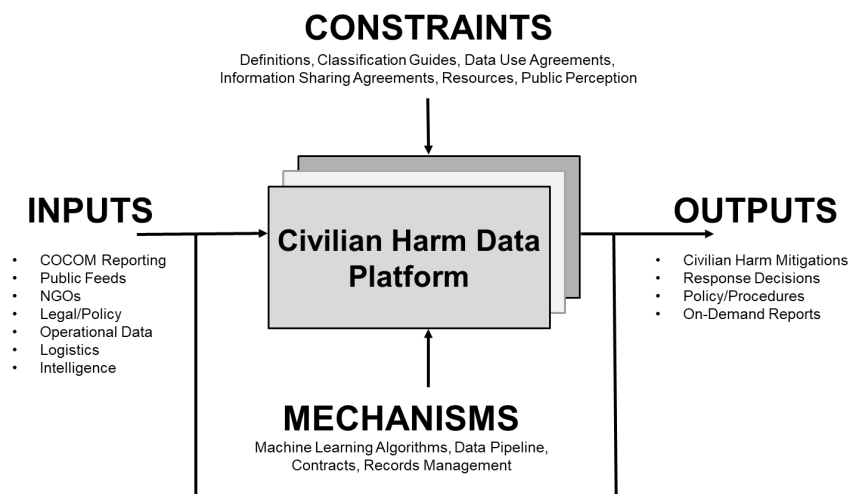


Figure 1. DMP ICOM Model

Findings

We clustered the findings into five topic areas, shown in Table 1. Each topic area hyperlinks to key findings and event discussions.

Table 1. CHMR OBJ6 TEM Topic Areas

Topic Areas	
1	<u>6f as a Foundational Milestone</u>
2	<u>Data Storage and Retention</u>
3	<u>User Roles and DMP Requirements</u>
4	<u>Indirect Effects</u>
5	<u>Prioritized User Stories</u>

Prioritized Actions

The participants identified the following as priority actions:

- Refine user stories based on event feedback.
- Define information requirements consistent with event findings. Include the following data characteristics: sources, types, existence, and completeness.
- Translate information requirements to DMP technical requirements.

Participants also identified follow-on actions necessary for continued progress:

- Receive a deep-dive briefing on the CASTLE system as an example federated system. The U.S. Army Special Operations Command (USASOC) Force Modernization Center (UFMC) originally developed this system for Civil Affairs uses.
- Engage the Defense Security Cooperation Agency to learn about their open source data ingestion and management practices.
- Request information from Office of the Under Secretary of Defense for Policy (OUSD(P)) on statutes of limitation for CH, data retention policies, and relevant records management requirements.
- Convene TEMs on sensitive activities (TS-Level) and multinational scenarios.

Proceedings

6f as a Foundational Milestone

Key Findings:

- Participants concurred that information requirements and data sources must be identified before subsequent Objective 6 items.
- Actions dependent on 6f include: defining and refining technical requirements (6g); selecting a platform (6h); providing DMP cost estimates (6i); developing policy change recommendations, legislative proposals, and other documentation updates (6h, 6k); standardizing CH reporting processes (6j) and DMP Standard Operating Procedures (SOPs) (6l); and developing DMP user training (6m).

CHMR-AP Action 6f calls for the joint proponent to develop and refine DMP information requirements and data sources. DMP information requirements and data sources must be established before any subsequent Objective 6 items can take place. It is critical that these information requirements and data sources are correct, as further actions will build on this foundation.

Additionally, identifying these information requirements and data sources allows a data and analytics response team (DART) to begin developing a minimum viable product (MVP).

Data Storage and Retention

Key Findings:

- The DMP requires OUSD(P) guidance on (1) the statute of limitations for making a CH claim, (2) DMP-related data storage policies, and (3) DMP-relevant records management.

The DMP requires access to authoritative data sources to inform investigations, perform analysis, and generate lessons learned. The DMP must also store this data consistent with

Department of Defense (DoD) and national data storage policies and retention requirements.

Participants also voiced concerns that, without appropriate guidance, differing data refresh rates and retention policies in source systems may lead DMP to compare data that was current at the time of an operation to data the DMP accessed post-event (e.g., at the investigation or analysis stage).

A final area of concern for participants was the interaction of declassification policies and retention requirements. For example, certain covert operations may be declassified 26 years after the fact. Participants questioned whether the DMP would be able to support investigations into civilian casualty (CIVCAS) reports and allegations 26 years after an event.

User Roles and DMP Requirements

Key Findings:

- Given that users require different levels of access to information within the DMP, the DMP must support role-based access.
- The DMP must, at a minimum, be capable of data ingestion and selective retention to enable fact finding and CH event validation.
- To facilitate non-biased analysis, the DMP requires access to data on non-events (i.e., CH claims known to not be credible due to, for example, a lack of military operations in the area), negatives (i.e., CH claims that were made but found to be not credible after investigation), and military operations where CH outcomes deviated from pre-operation estimates.

Users drive DMP information and functionality requirements. Participants identified at least four main user types that will access or inform the DMP: (1) CCMD users providing operational data and/or accessing the DMP to assess CH claims, (2) investigating officers (IOs) performing CH investigations, (3) Civilian Protection Center of Excellence (CP CoE) users generating CHMR-related reporting and lessons learned, and (4) civil and/or public affairs personnel responding to CH claims.

Participants noted that combatant commanders have the authority to place CHMROs where they see fit, and there have been stark differences in the approaches. For example, some place CHMROs with their safety officers, while others place them with public affairs. Participants advocated against directing command placement of CHMROs but did think that additional guidance on the actions CHMROs typically engage in might be useful for commanders.

Indirect Effects

Key Findings:

- Indirect effects are ill-defined. A common definition is needed prior to considering their inclusion in the DMP.
- Though direct economic impacts are in scope for the DMP, indirect effects may not be a priority for a DMP MVP. In the medium-to-long term, the DMP may need to ingest data indicative of indirect effects of military operations.

Military operations may generate indirect effects, such as economic, environmental, or other impacts. Participants sought clarity on whether these indirect effects are in scope for the DMP, and if so, how they should be treated within the platform. Participants also highlighted the challenge of obtaining intelligence, surveillance, and reconnaissance (ISR) resources needed to confirm indirect effects and temporally situate them relative to military operations.

Prioritized User Stories

Key Findings:

- Given their complexity, the Cyber Operation and Multinational Operation user stories, may merit follow-on TEMs.
- Refining the Cyber Operation, False Claim, and Multinational Operation user stories will ensure they remain realistic and within scope as defined by the CHMR-AP and the Draft CHMR Department of Defense Instruction (DoDI).

User stories are the mechanisms that help define DMP information requirements, establish core DMP functions, and identify critical data sources. The IDA team presented five categories of user stories to illustrate how different users might interact with the DMP across the data life cycle stemming from different military operations: Targeting, Cyber Operation, False Claim, Multinational Operation, and Troops in Contact. Participants discussed the Targeting, Cyber Operation, and False Claim user stories in detail. All military operations described in the user stories were situated during hostilities. Other characteristics varied to illuminate different data feeds, processes, and systems. Table 2 illustrates the different elements present in each user story, and Figure 2 displays the user stories as presented. Additional user story details and participant feedback follows.

Table 2: User Story Characteristics

User Story	CCMD	Engagement	Response	Responsibility Determination	Submission Mechanism
Targeting	AFRICOM	Kinetic	Ex Gratia	Affirmative	News/NGO
Cyber Operation	CYBERCOM	Non-Kinetic	None	Affirmative	News
False Claim	CENTCOM	None	Public Report	Negative	Public Access
Multinational Operation	PACOM	Kinetic	Ex Gratia	Negative	Public Access
Troops in Contact	CENTCOM	Kinetic	Ex Gratia	Affirmative	Self-Report

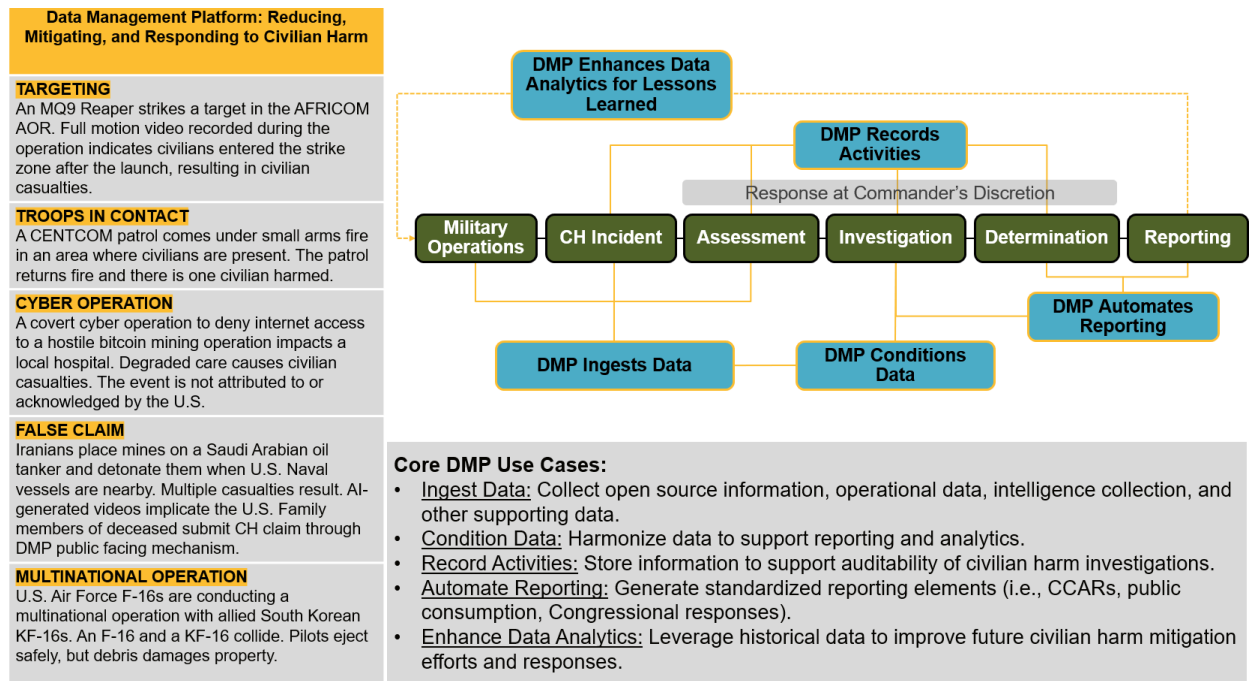


Figure 2: User Stories as Presented

Targeting User Story: AFRICOM identifies a target of interest. Intelligence collection informs target development and validation. The target is struck by an MQ9 Reaper in a pre-determined engagement area. Nearby civilians unexpectedly drive into the target area after missile launch but before impact. This results in CIVCAS. The operators complete a

combat assessment, and the strike is captured on full motion video as are visuals of civilians fleeing the strike site. The CCMD initiates an investigation and monitors reporting for indications of CIVCAS. Public news outlets report civilian casualties, and social media postings parallel this information. The DMP records the CIVCAS allegation, CCAR progress, and the ultimate CIVCAS determination. The allegation is found to be credible. The Commander recommends a response, which AFRICOM acts on. The DMP records this response and outputs a standardized report. The DMP facilitates lessons learned, which can be leveraged to inform and enhance future military operations.

Targeting User Story Feedback:

- Participants noted that many of the feeder systems do not retain snapshots of how the data appeared when the targeting package was prepared. This can be resolved by ensuring the DMP archives data itself or by creating a standard for data retention in feeder systems.
- In some targeting cases, CIVCAS is expected but deemed acceptable for a given target. DMP should consider nuances such as more/less CIVCAS than expected based on prediction models. However, prediction models for CIVCAS frequently are designed to be conservative and may not be suitable for this sort of analysis.
- The DMP would require access to Joint Prioritized Targeting Lists and No Strike Lists.

Cyber Operation User Story: The U.S. is engaged in hostilities against a terrorist group. U.S. intelligence indicates the group mines bitcoin to fund its weapons procurement and other activities against U.S. interests. The President directs USCYBERCOM to enact a covert cyber operation that takes the local Internet service provider offline and denies Internet connectivity to the bitcoin mining facility. However, there are unanticipated cascading effects that cause a local hospital to lose access to electronic medical records and Internet-enabled medical equipment. Dozens of civilians cannot receive proper care. Many degrade in medical condition, and some die as a result. The U.S. government does not acknowledge its responsibility for the cyber operation. Though CIVCAS resulted, no allegations are made due to the lack of attribution. USCYBERCOM systems record engagement authority, operational data, and operational outcomes—some of which the DMP ingests. USCYBERCOM investigative entities access this information in the course of an after-action review, generate a lessons-learned document, and ingests these lessons learned into the DMP to inform future operations. The DMP disposes of data as appropriate to comply with information distribution and records management requirements.

Cyber Operation User Story Feedback:

- Any CYBERCOM operation would need to be cleared through the CCMD for the affected area of responsibility (AOR). They would also be involved in any sort of response.
- Second- or third-order effects, such as the one described, are often difficult to detect given ISR resources available to commanders.
- All of the activity for this example would be at the TS/SCI or special access program (SAP) level.
- Many operations (not just cyber) are automatically declassified after 25 years. Will the DMP be able to handle allegations of CIVCAS at the 26-year mark?
- Special operations and cyber operations need specific follow-up actions at a higher level of classification to flesh out concerns regarding sensitive operations.
- The draft version of the DoD Instruction (DoDI) included some discussion about cyber operations; as written, cyber operations with kinetic effects, such as the one described, would be included in the DMP's scope.

False Claim User Story: Iranian naval vessels, U.S. Navy (USN) vessels, and Saudi oil tankers are present in the Strait of Hormuz. Iran places a charge on a Saudi oil tanker and detonates it as a USN vessel passes. All inventory and crew are lost. Subsequent reporting and social media postings circulate video showing USN vessels kinetically engaging the Saudi oil tanker. Soon thereafter, family members submit civilian harm claims through the DMP public access site. The U.S. government initiates an investigation in response and uses the DMP to record the allegation, investigation proceedings, and data generated by the investigative process. The Central Command (CENTCOM) investigating officer (IO) accesses the DMP searching for operational data (i.e., ISR, munitions data) that may indicate whether the USN vessel engaged kinetically. The IO finds no indication of kinetic activity. A digital forensics investigation indicates videos circulating online that appear to be AI generated. The DMP stores these findings, generating both secret-level and unclassified reports reflecting the lack of evidence that the U.S. was involved.

False Claim User Story Feedback:

- All the data the IO would need for this scenario is in a U.S. Naval Forces Central Command (NAVCENT) system.
- Participants pointed out that there would additionally be information from other ships in the area and possibly interviews with survivors rescued by the USN vessel.
- Who will have the expertise to lead the digital forensics investigation into the videos disseminated online?
- Are responses to misinformation and disinformation within scope of CHMR responses available to the CCCR?

Multinational Operation User Story: U.S. Air Force (USAF) aircraft are conducting a multinational operation with allied South Korean forces (KF) in the Indo-Pacific Command (INDOPACOM) region during the conduct of hostilities. USAF F-16 and KF-16 collide over South Korean territory. The USAF F-16 crashes in an agricultural area near Osan Air Base. Both pilots eject safely and file an incident report. Local news outlets report that debris damaged a Korean farmer's crops and farming equipment. A Korean civilian submits a CH allegation through official channels (i.e., a public access site hosted by the DMP). An investigation is conducted, and the DMP records its progress. The IO draws on black box data, radio recordings, and radar information to validate that the incident was an accident in the course of operations. These data objects offer critical data elements—such as date, time, and geolocation—to substantiate the Korean farmer's claims. The IO determines the allegation is credible, records this finding in the DMP, and recommends a payment to the farmer. The Commander actions this response and records it in the DMP. The DMP automatically generates an unclassified report walking through incident occurrence, investigation, and response. This report is shared with the U.S. Embassy in Seoul and is posted on the Embassy website to acknowledge the incident.

Multinational Operation User Story Feedback:

- Multinational operational scenarios more typically involve one country on the ground calling in air support from a second country. How could the DMP facilitate IO officer access to systems not necessarily owned by the U.S.?
- How does the DMP's need for auditable, authoritative data interact with, for example, the EU's "right to be forgotten"?
- We need a follow-on session to unpack this scenario in particular.

Troops in Contact User Story: A U.S. Army patrol is in the CENTCOM AOR during the conduct of hostilities. While returning from a key leader engagement, the patrol is attacked with direct-fire weapons. The patrol returns fire, and the adversary retreats. One civilian, present in the area of operations, is injured. When back from patrol, the Unit Commander—following appropriate chain of command—completes a standardized combat assessment and submits it through appropriate channels. The DMP records this assessment. The DMP performs text analytics and flags the report as a potential CH incident due to the mention of one CIVCAS. An investigation takes place and the IO records the progress and results in the DMP. The Commander decides on an appropriate response, which is also recorded in the DMP to enable automated reporting.

TEM Participants

- SES Adam Nucci, HQDA, G/3-5-7
- COL Steven Gandia, HQDA, G/3-5-7
- SES Dan Jensen, U.S. Army Analytics Group
- Leila Green, DAMO-SSP
- Edward Lescher, CP CoE
- Shawn Sumter, CP CoE
- Russell “Smack” Bedford, AF A2/6DO
- Avinash Ferrao, Army CIO
- Regina McCoy, CDAO
- Ellis Schmuck, DIA
- George Udeagbala, DSCA
- Janna Mantua, IDA for OUSD(R&E)
- Michael Ellis, J3
- Cameron Taylor, JTCG/ME
- Robert Stewart, Oak Ridge National Labs
- Curtis Stamps, OUSD(A&S)
- Elena Crespo, OUSD(P)
- Michael Goyette, USCYBERCOM
- Robert Lewis, USN
- Robert Tisdale, Fires Center of Excellence (Virtual)
- Jon Concheff, NORTHCOM (Virtual)
- Mark Miller, SOCOM (Virtual)
- Dwight Utley, SOCOM (Virtual)
- Michael Beavin, SOUTHCOM (Virtual)
- John DeMaso, SOUTHCOM (Virtual)
- Tom Johnson, SOUTHCOM (Virtual)
- Dennis Cahill, USASOC (Virtual)
- Mike Avey, CTR
- Laura Odell, IDA Assistant Director
- Cameron DiLorenzo, IDA
- Cliff Bridges, IDA
- Miranda Seitz-McLeese, IDA
- Todd Sabala, IDA
- Claire Haas, IDA

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YY) 00-08-23		2. REPORT TYPE Final		3. DATES COVERED (From – To)	
4. TITLE AND SUBTITLE Civilian Harm Mitigation and Response Action Plan (CHMR-AP): Objective 6 Results and Transition Plan				5a. CONTRACT NUMBER HQ0034-19-D-0001	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBERS	
6. AUTHOR(S) Laura A. Odell, Clifford M. Bridges, Cameron D. DiLorenzo, Claire E. Haas, Todd D. Sabala, Miranda G. Seitz-McLeese				5d. PROJECT NUMBER BC-5-4826	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES Institute for Defense Analyses 730 East Glebe Road Alexandria, VA 22305				8. PERFORMING ORGANIZATION REPORT NUMBER IDA Product 3000981	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Adam J. Nucci, Principal Director, Policy Resources & Analysis HQDA OCIO Pentagon 5C249, Washington, DC 20301				10. SPONSOR'S / MONITOR'S ACRONYM	
				11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution Statement A. Approved for public release: distribution is unlimited.					
13. SUPPLEMENTARY NOTES Project Leader: Laura A. Odell					
14. ABSTRACT On August 25, 2022, the Department of Defense (DoD) released its Civilian Harm Mitigation and Response Action Plan (CHMR-AP) to improve strategic outcomes, optimize military operations, and strengthen DoD mitigation of civilian harm through a reinforcing framework. Objective 6 (OBJ 6) of the CHMR-AP tasks the Secretary of the Army with developing a data management platform for CHMR-related data. This report documents OBJ 6 activities completed to date by the OBJ 6 Working Group, led by HQDA G-3/5/7, and a recommended plan for remaining activities.					
15. SUBJECT TERMS Data Management, Civilian Harm Mitigation, Data Platform					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Unlimited	18. NUMBER OF PAGES 122	19a. NAME OF RESPONSIBLE PERSON Adam J. Nucci, Principal Director, Policy Resources & Analysis
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (Include Area Code) 571-256-8924

