Research Brief

RAND NATIONAL DEFENSE RESEARCH INSTITUTE

Should Global Force Management Information Be Classified?

RAND RESEARCH AREAS
CHILDREN AND FAMILIES
EDUCATION AND THE ARTS
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INFRASTRUCTURE AND TRANSPORTATION
INTERNATIONAL AFFAIRS
LAW AND BUSINESS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
TERRORISM AND HOMELAND SECURITY

The Department of Defense (DoD) needs detailed information about the personnel and equipment in military units for planning and analytic purposes. The military services have such information but keep it in different formats on disparate systems, often with labeling specific to a given service. All this makes it difficult for DoD to gather information quickly. As a result, DoD has initiated the Global Force Management Data Initiative (GFM DI), a set of standards and protocols (but not a database per se) that makes it easier to share information. Most of the information is unclassified and is therefore already available on DoD's unclassified Internet system. However, potential adversaries have repeatedly penetrated DoD's unclassified Internet, raising the question of whether GFM DI data should be confined to DoD's classified system.

The Joint Staff asked the RAND National Defense Research Institute (NDRI) to make a recommendation about the need to classify GFM DI data. NDRI researchers approached this task in two steps. First, they developed criteria to determine why any information should be classified. Armed with these criteria, the researchers then took up the issue of classifying GFM DI information.

Why Classify Information?

The only reason to classify information is the belief that, if potential adversaries get it, they can use it to undermine U.S. security. The decision to classify information is not a trivial one because deciding to do so imposes important costs. Some are monetary, since classified material requires additional administration, storage, and handling. But other costs are arguably more telling because classification makes it more difficult to do business within or between government agencies and also potentially denies the public information.

To get a handle on the potential damage from an adversary's getting specific information, researchers developed the following four criteria for assessing whether it is worth classifying any particular piece of information:

- Does classification decrease the amount of information going to potential adversaries?
- Does the additional information adversaries would have if it is not classified affect what they know, and does it move them closer to the truth?
- How likely is this change in knowledge to affect adversary decisions, and does it do so in ways that help the adversary?
- Would the decisions the adversary makes based on such knowledge damage U.S. security?

Classifying information is warranted only if all four criteria apply:

- *only* if the failure to classify information means that an adversary is more likely to get it
- *and* if having it changes the adversary's estimate of a key piece of knowledge
- *and* if the change in knowledge is likely to alter a decision
- *and* if the decision is adverse to the United States.

Key findings:

- The Department of Defense routinely gathers information on its own military force structure.
- Currently, analysis is difficult because the information is scattered and heterogeneous.
- The Global Force Management Data Initiative (GFM DI) will ease combining such information.
- Some worry that potential adversaries can exploit the information and therefore want it stored on classified systems.
- RAND researchers found no reason to classify GFM DI information as a whole but suggest that some subsets may warrant additional protection.

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of published, peer-reviewed documents.

Corporate Headquarters
1776 Main Street
P.O. Box 2138
Santa Monica, California
90407-2138
TEL 310.393.0411
FAX 310.393.4818

Even if all these conditions are met, classification is merited only if its costs are lower than the likely adverse effects of keeping the information unclassified.

What Is GFM DI, and What Is New About It?

GFM DI makes force authorization data—the personnel and equipment that a unit is allowed to have but will not necessarily deploy with—accessible. Such data, however, should not be confused with what potential adversaries may really be interested in: the personnel and units that are both on hand and available for war. These are almost always less than what is authorized. Authorization data are, at best, a proxy for the latter.

GFM DI is not a database and does not require creating new ones. What it does require is that the services provide a minimum set of data about their force elements. GFM DI helps integrate service force data by enabling users to access what used to be separate sources as if they were a single, coherent database. Security concerns revolve around the broader sharing of data or the aggregation of different types of data as a result of the initiative.

Does GFM DI Pose a Security Risk?

The security concerns GFM DI raises rest on the potential for nefarious actors—both state and potentially nonstate—to use its data. NDRI researchers framed these concerns as three questions:

- Will GFM DI give adversaries information they would not otherwise have?
- Will GFM DI make it easier for adversaries to confirm information they already have?
- Will GFM DI's aggregation capabilities create new security vulnerabilities?

For each question, researchers determined how the changes that GFM DI might require or possibly induce would affect the access potential adversaries might have to such data. They then examined the data types included in the initiative and asked whether the classification or other restrictions on it were supported, based on the four criteria above.

The upshot of this analysis was that, for the minimum data set, researchers found no good reason to classify GFM DI as a whole. Concerns about standardization, directed generation of the minimum data set, and broader use of force structure data appear unfounded. With respect to how much potential adversaries might learn about the overall U.S. force structure, researchers concluded that the change was from many alternative sources of information to somewhat better data. Generally, concerns failed at least one of the four criteria for classifying information.

However, researchers noted that two concerns merit consideration. One stems from the aggregation of information about platforms, units, and personnel billets associated with them. For example, it might be possible to discern sensitive information about a particular unit from the fact that it requires billets of a minimum clearance level. This information might suggest that what appears to be an ordinary unit is not. A second, greater risk occurs when billets can be tied to individuals through links to other databases. This can occur because the same identifier used in GFM DI also appears in personnel databases to indicate which billets an individual occupies and has occupied in the past. Personnel databases also contain other information, such as location and family, that could be exploited.

Recommendations

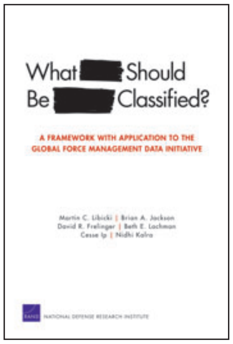
Although NDRI researchers advised against classifying GFM DI data, they made four recommendations to deal with residual security concerns.

First, be cautious when creating additional fields or when adding data beyond the minimum set. Someone (e.g., on the Joint Staff) should periodically review GFM DI looking for information that should not be there.

Second, the list of displayed fields and allowable attributes may need to be trimmed. Listing security classifications of billets or special requirements, such as language capabilities, may increase the risk to individuals or expose more about a unit's purpose or capabilities than is prudent. These characteristics could be dropped or masked by aggregation or with neutral labels.

Third, consider classifying information on units, platforms, or activities that guard their security through obscurity. The data integration available through GFM DI inherently puts such strategies at risk. That said, data-mining techniques pose similar risks in other venues, and prudent planners need to account for them.

Fourth, study the mutual effects between GFM DI and personnel databases in greater detail. The ability to link a person to a billet and a billet to a unit may reveal more about the unit than anything in GFM DI could. These links could open the possibility of social network analysis. The extent of this threat is unclear and thus warrants additional analysis. ■


What [redacted] Should
Be [redacted] Classified?
A FRAMEWORK WITH APPLICATION TO THE GLOBAL FORCE MANAGEMENT DATA INITIATIVE
Martin C. Libicki | Brian A. Jackson
David R. Frelinger | Beth E. Lachman
Cesse Ip | Nidhi Kalra
NATIONAL DEFENSE RESEARCH INSTITUTE

This research brief describes work done for the RAND National Defense Research Institute documented in *What Should Be Classified? A Framework with Application to the Global Force Management Data Initiative*, by Martin C. Libicki, Brian A. Jackson, David R. Frelinger, Beth E. Lachman, Cesse Ip, and Nidhi Kalra, MG-989-JS (available at http://www.rand.org/pubs/monographs/MG989/), 2010, 110 pp., $20, ISBN: 978-0-8330-5001-4. This research brief was written by Jerry Sollinger. The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.

RAND Offices
Santa Monica, CA • Washington, DC • Pittsburgh, PA • New Orleans, LA/Jackson, MS • Boston, MA • Doha, QA • Cambridge, UK • Brussels, BE