

POLICIES OF FEDERAL SECURITY LABORATORIES

Susannah V. Howieson

The Problem

The Departments of Defense, Energy, and Homeland Security fund and/or operate about 80 facilities, including laboratories that focus predominantly on national security matters or “federal security laboratories.” IDA assessed various aspects of the Federal security laboratories, including infrastructure, governance structures, and personnel policies, seeking ways to strengthen the enterprise.

Facilities and Infrastructure

The federal security laboratory system comprises thousands of buildings and other structures, many of which are decades old and have not been refurbished. Aging and deteriorating facilities and infrastructure (F&I) may threaten the ability of federal agencies to sustain high-quality research in support of their national security missions. Given these concerns, IDA was asked to pilot an effort to better understand F&I planning, prioritization, and assessment at ten selected federal security laboratories.

Through a literature review, discussions with agency and laboratory personnel, and a workshop, the IDA research team identified four areas critical to federal security laboratory F&I: planning processes, prioritization criteria, stakeholder involvement and communication, and data and metrics.

Planning Processes

Federal security laboratory F&I staff lack agency and laboratory leadership support in defending the need to maintain, upgrade, and construct new F&I. As a result, there is no integrated plan to address long-term F&I needs across the agency and the national security enterprise. In addition, annual budget decisions and F&I reporting requirements are not linked with a strategic vision and investment strategy. Department of Defense (DoD) laboratories face the additional constraint of their F&I needs being prioritized against other types of F&I and military needs, such as schools, hospitals, and barracks. Laboratories from all agencies reviewed have encountered barriers to using alternative financing mechanisms for F&I projects.

Strategies to address these challenges include leveraging resources through partnerships, setting aside funding in the agency’s annual budget for large F&I projects specifically for laboratories, and using a combination of in-house capability and external architectural and engineering firm expertise.

Properly maintaining and constructing F&I make up an important element of the ability of the Federal security laboratories to support mission-critical capabilities.

Prioritization Criteria

Federal security laboratories prioritize F&I plans using a set of criteria based on their impact on the mission, health and safety, security, environmental compliance and zoning, energy usage and sustainability, costs and building conditions, and resource leveraging within and across laboratories. To track progress, the criteria are assessed using metrics. However, the criteria and metrics used at the agency level sometimes do not fully capture the F&I impact relative to the agency's mission because F&I staff frequently are not included in developing agency level criteria and metrics. Moreover, agencies typically develop F&I prioritization criteria in a top-down fashion. This is particularly challenging for DoD's federal security laboratories since their F&I funds are part of the much broader Military Construction (MILCON) program.

Some Federal agencies and laboratories have recently incorporated various strategies into developing F&I prioritization criteria and frameworks: using data-driven and qualitative methods to evaluate criteria, involving laboratory representatives in developing new criteria, assigning weights to prioritization criteria, and using a decision-gate approach for assessing the F&I portfolio.

Stakeholder Involvement and Communication

Multiple stakeholders are involved in the F&I planning, prioritization, and assessment processes, including the researchers and managers at the laboratories; research customers; a wide variety of firms that provide facilities services,

such as architectural and engineering firms; state and local governments; Congress; executive offices, such as the Office of Management and Budget (OMB); state and federal environmental and safety regulators; and local communities.

The scientists, engineers, and laboratory management who conduct and oversee research activities must be able to communicate their F&I needs to the organization's F&I management staff and the overall Department and agency leadership. A major challenge is the lack of communication among stakeholders: those internal to the laboratory can have conflicting priorities given highly constrained funding; at intermediate levels there are disconnects between the laboratory itself and various oversight bodies; and at higher levels there are difficulties getting the attention of and priority consideration from the Departments and agencies, OMB, and Congress. Part of the problem is that laboratories individually pursue their own F&I needs and tend not to collaborate well to communicate their collective enterprise requirements.

IDA researchers identified four strategies that could improve the communication across the laboratories, agencies, and relevant F&I stakeholders: agencies could coordinate with their laboratories to develop a clear strategic vision; laboratories and agencies could develop communities of practice; laboratory F&I managers could interact with researchers in the planning and implementation of F&I and equipment; and laboratories could establish timely mechanisms to communicate with F&I-related stakeholders.

Data and Metrics

There are several challenges to using data and metrics within F&I investments. Assessments are expensive, time-consuming, and irregularly conducted. Some agencies and laboratories validate F&I data only every few years, using estimates between the years that inspections are performed. Finally, there is reluctance to share data to permit benchmarking because of the possibility that it could place laboratories at a disadvantage when competing for F&I funds or customers.

Strategies to address these challenges include providing high-level guidance to define, collect, and maintain metrics; standardizing metrics and data elements across laboratories; and engaging in benchmarking and other data-sharing efforts.

Next Steps for Facilities and Infrastructure

Based on the strategies already adopted by some laboratories and on the suggestions provided by workshop participants and interviewees, five broad recommendations were proposed:

1. Establish and participate in an interagency forum for sharing best practices.
2. Facilitate F&I planning processes and funding.
3. Establish standard criteria and methods to prioritize F&I investments.
4. Expand opportunities to involve stakeholders and improve communications.

5. Improve the collection, quality, and use of data and metrics.

Laboratory Governance

Federal security laboratories have different missions, research portfolios, budgets, and communities of sponsors and users. They also embody a mix of governance types:

- Government-Owned/Government-Operated (GOGO) laboratories, which are run by government employees and operate under varying organizational, administrative, and research arrangements established by parent agencies
- Federally Funded Research and Development Centers (FFRDC), which are run by private-sector organizations and maintain close, long-term relationships with government sponsors, within a structured regulatory environment, some of which are Government Owned/Contractor Operated (GOCO) facilities
- University Affiliated Research Centers (UARC), which are run by universities and share some but not all of the attributes and regulatory environment of FFRDCs.

IDA was asked to address the following questions related to Federal security laboratories: What are the critical trends facing Federal security laboratories today? How does governance structure relate to the operation and performance of research and development (R&D) that supports the national security missions? How can the Federal government best support the Federal security laboratories to address future national security challenges?

To assess these questions, IDA researchers organized expert panels composed of former and current federal security laboratory directors; department and agency headquarters personnel; and laboratory leaders from other federal laboratories, academia, and industry.

Trends Affecting Federal Security Laboratories

The panel sessions focused on the overarching trends that have affected R&D activities or performance at the federal security laboratories: personnel-related challenges, competition from R&D entities in foreign countries, changes to laboratory research focus and funding, and increases in regulatory requirements and oversight.

Current personnel challenges for federal security laboratories are the result of several long-term trends, including competition from the private sector, an aging workforce, and waning numbers of appropriately educated and security-clearance eligible young scientists. These trends led panelists to express concerns over the ability of the federal security laboratories to maintain a high-quality workforce.

Questions were raised about the ability of the federal security laboratories to compete with the private sector for high-quality talent, particularly in certain high-demand fields, such as cyber security. There are increasing numbers and proportions of foreign-citizen undergraduate and graduate students in U.S. academic institutions who are not eligible for security clearances. Student recruitment is key to maintaining the federal

security laboratory workforce, and increases or improvements to existing student recruitment programs were recommended by the panelists.

Competitive salaries also present a challenge to recruiting employees. In particular, if GOGO laboratories had more flexibility in their personnel management systems, panelists believed the labs would likely improve their ability to recruit and retain scientists and engineers.

Panelists expressed concern about the reduced opportunities for laboratory researchers to interface with foreign-based researchers and internationally located industry collaborators. In particular, scientists at federal security laboratories were said to have difficulty collaborating with researchers overseas due to security requirements and current budget pressures to reduce travel for conferences and peer engagements.

Panelists were also concerned that emerging national security fields such as cyber security, information technology, quantum computing, bioterrorism and bioweapons, and nanotechnology have not been adequately addressed by federal security laboratories.

Two funding issues were seen by panelists as challenging DoD and Department of Energy (DOE) laboratories' ability to conduct their research—the increasing fragmentation of budgets and reliance on shorter-term rather than long-term programmatic funding. In addition, prior policy decisions have led laboratory directors to rely on outside funding support to maintain core capabilities due to declining overall budgets.

Panelists were also concerned that federal security laboratories face more regulatory requirements related to safety than non-federal laboratories, which increases the levels of bureaucracy and raises the regulatory burden on laboratory researchers. Increases in regulatory requirements often represent the cumulative effects of multiple remedial actions, each one taken in response to a single incident that was considered a liability to the laboratories or their sponsor agencies. This has an adverse effect because there is a perceived level of distrust between the agency offices and the laboratory staff conducting research.

Laboratory Roles and Governance Structures

Panelists reached four conclusions regarding laboratory roles and governance. First, federal security laboratories fulfill a unique role in U.S. national security research and development. Second, each governance model has certain advantages. Third, critical laboratory characteristics do not necessarily depend on their governance structure. Finally, both exemplar and sub-standard examples of laboratories exist under each governance model.

According to panelists, wholesale transition of all federal security laboratories from one governance structure to another is not advisable or warranted, but the best attributes of each governance structure could be incorporated into others. The general view was that the costs associated with transitioning all federal security laboratories to one governance structure would far outweigh the benefits. Panelists believed that such

changes in management are disruptive and could leave lasting negative impacts. Thus, panelists recommended practices to facilitate the expanded use of the best laboratory attributes at all federal security laboratories. The primary recommendations derived from discussions with the panelists are:

- Rationalize the oversight burden on the laboratories
- Maintain or reinstitute laboratory flexibility for research budgeting
- Increase or maintain autonomy and accountability in personnel systems, particularly in GOGO laboratories.

Personnel and Workforce

IDA has performed a number of research projects addressing the national security science and technology federal workforce, including efforts focused on hiring foreign scientists and engineers at federal security laboratories, personnel exchanges, industry hiring best practices, uniformed scientists and engineers, and federal science, technology, engineering and mathematics (STEM) workforce quality. The first two of these projects are discussed in more detail below.

Hiring Foreign Scientists and Engineers at Federal Security Laboratories

There are increasing numbers and proportions of foreign-citizen undergraduate and graduate students in U.S. academic institutions who are incapable of obtaining security clearances. Non-U.S. citizen doctoral graduates with temporary visas are

outpacing U.S. citizen and permanent resident doctoral graduates in national security science and technology fields at U.S. academic institutions, and more than one-half of PhDs awarded by U.S. engineering schools are earned by non-U.S. citizens.

However, it is not easy for new foreign-born, U.S.-educated, STEM researchers to work at federal security laboratories after graduation because of their citizenship and the difficulty in obtaining a security clearance. Hiring foreign nationals at federal security laboratories is challenging because the work could involve handling classified information, which may not be accessed by workers without U.S. citizenship and security clearances. Further limitations stem from recent changes in appropriations law stating that DoD cannot compensate a noncitizen, unless the noncitizen is lawfully admitted for permanent residence.

IDA helped organize and assess the results of a Government workshop convened to address these issues with representatives from multiple elements of DoD, U.S. Citizenship and Immigration Services, OMB, and the Domestic Policy Council. Subsequently, a working group was established to articulate clear paths for foreign national students studying in the United States to remain in the United States and for exceptional foreign national scientists and engineers to apply for employment at a DoD federal security laboratory and gain U.S. citizenship.

IDA supported the working group by providing background materials on immigration pathways,

investigating hiring authorities, and analyzing processes available to DoD to provide foreign citizens with access to classified materials when needed. Also, we supported the development of a guidance document that outlines existing laws and regulations and clarifies current processes and procedures for employment, immigration, and granting foreign national scientists and engineers at DoD laboratories access to classified materials when eligible and qualified U.S. citizens are not available.

Personnel Exchanges

While mechanisms, such as Intergovernmental Personnel Act agreements exist for personnel exchanges between the federal security laboratories and other science and engineering, academic, and industrial organizations, they face numerous challenges, including lack of awareness of exchange opportunities and ineffective advertisement to both government personnel and outside organizations; the length and complexity of the application process; resource constraints, including unwillingness to give up valued personnel; and uncertainty over the impact on one's career and transition back to the original organization. There are also a number of legal and regulatory requirements intended to prevent conflicts of interest during and after a personnel exchange that can impede the establishment of personnel exchanges.

IDA researchers identified currently available personnel exchange mechanisms, particularly those open to for-profit organizations; investigated the exchange process

at different organizations; described the roles exchange personnel fulfill; analyzed the potential benefits of personnel exchanges; summarized barriers to utilizing personnel exchange mechanisms; and developed policy options for improving existing mechanisms or creating new ones.

Preliminary results pointed to a number of policy options for improving current personnel exchange mechanisms:

- Create high level executive encouragement and support for personnel exchanges
- Streamline the agreement package and process and issue exchange procedure manuals
- Create a government-wide central repository for lists of opportunities and required paperwork
- Establish reciprocal exchanges so that organizations maintain the same number of employees
- Engage a larger group at each agency to lead to a collective commitment to an exchange program

- Establish agency-wide personnel exchange funds
- Make a commitment to employees participating in exchanges that their career trajectory will not be impeded by the exchange.

In addition, options were presented for specifically engaging for-profit exchanges. Since DoD has multiple programs for sending individuals to industry, the recommendations focused on new methods for temporarily bringing for-profit personnel into the government:

- Establish a pilot program for industry rotators in DoD
- Draft a legislative proposal establishing authority for DoD to utilize industry exchanges.

Ms. Howieson is a Research Staff Member in IDA's Science and Technology Policy Institute. She holds a Juris Doctor from Boston University School of Law and a Masters of Environmental Management from Duke University.