Balancing Security and Knowledge Sharing

BY RYAN AVERBECK, JOHN DAY, AND G. A. GADDY

The Fall 2007 issue of *ASK Magazine* generated a lot of discussion among those of us involved in the NASA Exploration Systems Mission Directorate (ESMD) Technology Protection Program. William Gerstenmaier's "On a Need-Not-to-Know Basis" made us ponder the overwhelming, ubiquitous onslaught of information that constantly bombards the NASA family. As he stated:

> During a single week in October 2006, the NASA Headquarters e-mail servers delivered approximately 1.25 million e-mails. With roughly 1,000 people at Headquarters, this works out to 1,250 messages per person. The nasa.gov domain has approximately two million distinct Web pages residing on its servers. This yields roughly thirty-two Web pages for every civil servant and contractor in the NASA family.

Viewed from an information-overload perspective, this shows just how much NASA information is exchanged, transferred, and requested on a daily basis. These same facts, viewed from a slightly different perspective, raise another question: How much of the information in this flood should in fact be protected? NASA, the world's premier space agency, often leads advances in space-related sciences and engineering. If NASA were a commercial entity, the knowledge possessed by civilians and contractors could be called proprietary information; in certain instances it would manifest itself as intellectual property, with the ownership rights that term implies. Thought of in this manner, the intellectual property is knowledge that gives NASA a competitive advantage in space sciences, engineering, and exploration.

NASA has a deservedly proud fifty-year history of sharing innovation at an astonishing rate. The National Aeronautics and Space Act of 1958, as amended, calls for "… the widest practicable and appropriate dissemination of information concerning its [NASA's] activities and the results thereof …." This same Act, though, also requires NASA scientists and engineers to

> … contribute materially to:
>
> The preservation of the role of the United States as a leader in aeronautical and space science and technology and in the application thereof to the conduct of peaceful activities within and outside the atmosphere;
>
> The preservation of the United States' preeminent position in aeronautics and space through research and technology development related to associated manufacturing processes …

The balancing act between sharing information and protecting it is further complicated by the 2006 National Space Policy, which states that space capabilities are vital to the nation's interests and the United States will "take those actions necessary to protect its space capabilities." Many of the requests for information that come to NASA come from foreigners.

To contribute to this balancing act, NASA's ESMD developed a Technology Protection Program and has devoted time and effort tailoring the program to specifically address NASA needs, charter requirements, and national strategies compatible with the current global environment.

To help mitigate the challenges associated with the establishment of the Technology Protection Program, ESMD enlisted our services to form the core of the Mission Critical Information (MCI) assessment team. The MCI assessment team is the "nervous system" of the ESMD Technology Protection Program. Ryan Averbeck's technology protection experience related to the Department of Defense and commercial sectors comes from an extensive background as a counterintelligence agent and service as an assistant director at the Army Research and Technology Protection Center (ARTPC). John Day is a board-certified security management professional and has extensive experience implementing security programs at NASA. G. A. Gaddy brings extensive experience and insight as a Department of Defense scientist, former National Academies of Science National Research Council postdoctoral fellow at Langley Research Center, and a senior technology protection engineer at the ARTPC. The team's experience proved critical in the development of the Technology Protection Program processes. Our varied backgrounds and experiences provided a multidiscipline foundation for NASA to develop and implement a unique, customized Technology Protection Program.

The ESMD Technology Protection Program process requires the impartial MCI assessment team to review and evaluate all pertinent technical aspects and documentation related to the research, components, systems, elements, projects, and programs under consideration. The team's analysis includes, but is not limited to, the daunting task of horizontal cross-referencing. This involves referencing technologies against the Militarily Critical Technologies List, the Developing Science and Technologies List, the export control criteria from the Department of State, and other sources. The MCI assessment team also conducts analysis to determine if research or technology under development is "state of the world" versus "state of the art," and revolutionary versus evolutionary.

For example, if NASA were developing a Pentium 4 processor and the rest of the world possessed Pentium 3 processors, the technology could be considered evolutionary in nature, since Moore's Law would lead us to believe the rest of the world would catch up with a Pentium 4 of their own in relatively short order. In this instance, the Pentium 3 processors are state-of-the-world technology, and the Pentium 4 is not a large enough order of magnitude improvement to be revolutionary or state of the art. If NASA were developing a Pentium 4 processor while the rest of the world possessed Commodore 64 processors, this technology would then be revolutionary since it represents orders of magnitude improvement.

After conducting technical discussions with NASA and contractor subject-matter experts, the MCI team presents its findings and recommendations to NASA management for an MCI determination decision. If information is designated mission critical, the team then works with NASA management and Technology Protection Program personnel to develop the appropriate procedures to protect it. Protection does not necessarily mean the information or technology cannot be shared or disclosed. In most cases, it provides the foundation for NASA management to make informed decisions regarding appropriate dissemination.

An MCI designation is not necessarily permanent. For example, during a recent assessment, a particular set of test results was deemed MCI by NASA management. This determination was largely based on the active steps a foreign entity was taking to obtain the information. When an acquisition decision was later made by NASA management to pursue another engineering solution, the MCI was no longer of great value to NASA or the foreign entity, so the Agency removed the mission-critical designation from the test results.

In light of the information overload problem described by Gerstenmaier, the Technology Protection Program assists in identifying and protecting NASA's information from unauthorized release or inadvertent disclosure. The team helps the NASA family understand and mitigate a multitude of concerns:

WITHIN THE SECURITY AND PROTECTION DISCIPLINES, ONE AXIOM ALWAYS HOLDS TRUE: THE BEST COUNTERMEASURE TO THREATS IS AN EDUCATED AND ENGAGED WORKFORCE.

- How much of NASA-controlled information is inadvertently released outside approved channels because employees are overwhelmed by volumes of information?
- How well-trained and equipped is NASA to "know" what would require protection? We are currently charged with protecting several categories of information such as export controlled, contractor proprietary, sensitive but unclassified, classified (such as confidential, secret, and top secret) information, and the recently codified MCI, just to name a few.
- Does the NASA team (civilians and contractors) understand the nature and capabilities of those that wish to obtain our controlled information via nefarious means or by simply exploiting our information overload? When was the last time employees requested or received a threat briefing from NASA counterintelligence?
- Are we adequately prepared and staffed as an agency to review thousands of pages of information to determine what should receive protection?
- What are the benefits and ramifications of controlling versus sharing critical NASA information?

The Technology Protection Program helps streamline information dissemination by giving the NASA workforce guidance on the limits of sharing particular information. Identifying the specific information that requires protection makes information sharing easier and clearer. One of the major factors in the success of the NASA technology-protection model is the MCI team's understanding of programs' cost, schedule, and performance drivers. The entire technology-protection team respects NASA's mission, history, and culture and works hard to minimize the impact of these essential security measures on programs. The program explains why particular information is of extreme value to the Agency and the nation and should not be shared outside established protocols. Within the security and protection disciplines, one axiom always holds true: the best countermeasure to threats is an educated and engaged workforce.

To promote education and awareness of the Technology Protection Program, the team participates in meetings, including project control boards, quarterly conferences, and the PM Challenge. The team also provides tailored briefings to project element scientists, engineers, and management. The team and NASA strive to put programs and projects in direct control of their technology-protection activities. ●

RYAN AVERBECK is currently a PhD candidate completing his dissertation in computer and information security at Northcentral University and works as a principal technical manager at Concurrent Technologies Corporation, where he develops and implements research and technology protection programs for government and industry clients.

JOHN DAY is the security operations manager for United Space Alliance at Kennedy Space Center, Florida, where he is responsible for security and access control for the Space Shuttle. He also is the program manager for the United Space Alliance/ Concurrent Technologies Corporation team for the NASA Technology Protection Program.

G. A. GADDY is the principal technical manager of the Technology Protection and Management Office at Concurrent Technologies Corporation in Huntsville, Alabama. He has been a researcher for the National Academy of Sciences' National Research Council at NASA Langley Research Center and a civil servant at the U.S. Army Research Laboratory.