DRAFT

NATIONAL ACADEMIES Sciences Engineering Medicine

National Science, Technology, and Security Roundtable

June 29, 2022 Open Session Summary

The National Science, Technology, and Security Roundtable of the National Academies of Sciences, Engineering, and Medicine convened three panels on June 29, [1]2022 to consider: (1) academic perspectives on promoting and protecting science and technology (S&T) research and advancing international engagement; (2) integrating U.S. government, private sector, and science-security experience; and (3) cybersecurity and research security.

In welcoming participants, Roundtable co-chair **Maria T. Zuber** (Massachusetts Institute of Technology) explained that the purpose of the sessions was to inform the development of a Roundtable workshop to consider approaches for securing and strengthening an open federally funded scientific research ecosystem. The workshop, entitled *Openness, International Engagement, and the Federally Funded Science and Technology Research Enterprise*, is scheduled to take place in August 2022.

Ten experts from the higher education and security communities made short presentations, which are summarized under each presenter's name below. Comments prompted by questions from Roundtable members during discussion sessions are attributed to the presenters under thematic headings.

ACADEMIC PERSPECTIVES ON PROMOTING AND PROTECTING SCIENCE AND TECHNOLOGY (S&T) RESEARCH AND ADVANCING INTERNATIONAL ENGAGEMENT

[1] This document is a draft summary of presentations and discussions from the open session of the June 29, 2022 meeting of the National Science, Technology, and Security Roundtable of the National Academies of Sciences, Engineering, and Medicine. The summary was prepared by science writer Paula Whitacre. It was prepared to stimulate discussion at the November 14-15, 2022 National Academies workshop on Openness, International Engagement, and the Future of the Federally Funded U.S. Science and Technology Research Enterprise. This document is not a report of the National Academies of Sciences, Engineering, and Medicine and has not been subjected to its review procedures.

Zuber moderated the panel, which consisted of **John Mester** (Universities Research Association [URA]), **Wendy Streitz** (Council on Governmental Relations [COGR]), and **Sarah Spreitzer** (American Council on Education [ACE]). Panelists were asked to consider four topics: (1) promoting and protecting U.S.-sponsored scientific research as a national security asset; (2) foreign engagement and access to foreign STEM talent; (3) accessing current and reliable relationships between scientists and security professionals; and (4) establishing relationships between scientists and security professionals.

John Mester

Mester noted he was sharing his own views and not necessarily those of the institutional members of URA, but that his comments were informed by two URA convenings on policy issues within the past year. The first was on building effective partnerships between national laboratories and universities, which included discussion about how to bridge the differences in culture between the two communities. The second was a set of discussions at the 2022 Council of Presidents meeting and previous board meetings on research security.

Striking a balance between security and openness is critical but difficult to achieve. While the academic community now has a better awareness of potential threats than previously, understanding the scope of the threats—not just that they exist—requires more effective, ongoing communication between the security and research communities. To achieve a balance, it is crucial to understand the contributions of the research enterprise to the nation's culture, economy, health, and national security. This includes an assessment of the impact of academic openness and collaboration on the success of the research enterprise. Within the scientific community, the value of open research is axiomatic. This is a problem because, since it is taken as a given, the value has not been articulated in a way that is convincing to those outside the research community.

It is appropriate to make the case that the open exchange of ideas, participation of diverse communities and international partnerships are critical to scientific achievement and U.S. scientific leadership. Some aspects are easy to quantify, such as that 1 in 5 entrepreneurs in the United States are immigrants, three-quarters of whom came to the United States as students. The large percentage of international students in science, technology, engineering, and medicine

(STEM) fields in U.S. universities leads to a large percentage of foreign-born S&T professionals in the workforce. A recent study by the National Bureau of Economic Research showed that, rather than crowd out U.S. students, international students increase opportunities for U.S. students, in part because they increase the resources available to universities.[2] Exposure to international students has also had a positive impact on the academic achievement of U.S.-born students.

Recent reports have indicated not only a decline in international students coming to the United States, but also that the United States is no longer the first choice for some students, in part because of increasing opportunities elsewhere, such as Germany and Canada. While it is too early to conclude if this is because of recent U.S. immigration policies, etc., it is important to consider the concept of time constants. That is, a decline in the perception of the United States as a beacon for scientific research can happen quickly and it may take many years to recover. Risks in the decline of an open research culture include a decline in workforce development, entrepreneurial success, universities' financial health, and new idea generation and cross-fertilization. Another aspect of open research is that, in many areas of discovery science, the United States is not the only player; in fact, due to the scale of effort required for advancement in some fields, some fields are inherently global.

The cost of regulatory approaches should not overwhelm the resources, both in terms of time and money. The efficacy of regulatory requirements is enhanced by a close dialogue between the security enterprise and universities and research centers. Universities need to understand what information is valuable for security, and the security establishment needs to understand the impact that requests will have on university partners. Fulfilling the requirements of new regulatory regimes will necessitate enhanced infrastructure and, in turn, increased indirect cost support. New security requirements should balance the varying response capacities of large and small universities. Large universities may have a greater capacity to deal with regulatory matters, but scientific innovation comes from a variety of places. Policies and processes that enable participation across the spectrum will be more effective. National Security Presidential

[2] J. Bound et al. 2021. The Globalization of Postsecondary Education: The Role of International Students in the U.S. Higher Education System. National Bureau of Economic Research Working Paper 28342, available at http://www.nber.org/papers/w28342.

Memorandum 33 (NSPM-33),[3] along with the memorandum's implementation guidance[4] and follow-up letters, have made a good start to address these issues, especially with regard to standardizing reporting requirements across funding agencies.

The full extent of diverse expertise must be developed and applied to develop a richer connection between research security and the research communities. To this point, Mester pointed to a recent NSF program solicitation on research security training for the U.S. research community.[5]

Mester is encouraged by robust discussion on the topic, including the Department of Justice announcement in February 2022 that the National Security Division is changing its strategy on academic research security cases and ending the China Initiative. He closed his remarks with a statement by Matt Olson, Assistant Attorney General for National Security at the Department of Justice, on the balance between security and openness. "Safeguarding the integrity and transparency of research institutions is a matter of national security, but so in ensuring that we continue to attract the best and brightest researchers and scholars to our country from all around the world, and that we all continue to honor our tradition of academic openness and collaboration."

Wendy Streitz

Streitz said she would echo similar themes to those of Mester, including the value of open research and collaboration to enhance national security and to ensure that the United States is not left behind. Principles enshrined in National Security Decision Directive 189 (NSDD-189) continue to be sound today, even with a new focus on research security.[6] Institutions have

[3] Presidential Memorandum on United States Government-Supported Research and Development National Security Policy. National Security Presidential Memorandum-33. Issued January 14, 2021, available at https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.

[4] National Science and Technology Council. 2022. Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development, available at https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.

[5] National Science Foundation. 2021. Program Solicitation NSF 22-576. Research Training for the United States (U.S.) Research Community, available at https://www.nsf.gov/pubs/2022/nsf22576/nsf22576.htm.

[6] National Security Decision Directive 189, National Policy on the Transfer of Scientific, Technical and Engineering Information. Issued September 21, 1985, its purpose was to establish "national policy for controlling the flow of science, technology, and engineering information produced in federally-funded fundamental research at

systems, processes, and training in place. But there is tension between security concerns by some federal agencies and the push for open access to research, including the underlying data, by other agencies. They seem to be going in two different directions, which is confusing to administrators and faculty.

Costs are real, and they are mostly administrative. Universities are disadvantaged among grantees to cover these costs since their indirect recovery rate was capped more than 30 years ago. New administrative requirements are absorbed by universities. This is not the case for industries, hospitals, state and local governments, or nonprofits. While steps are needed to enhance security, it is important to understand the burden in financial costs and people-hours, especially for small and mid-sized institutions. Some, including minority-serving institutions, cannot institute processes and hire people, and thus may not be able to afford to participate in federally funded research.

Progress has been made in recent years. Streitz noted the effort by the FBI to understand academic culture and to publicly acknowledge how far universities have come. COGR has some resources on this topic, but there is more work to do.[7] Universities do not have the tools and information to assess a specific threat, nor should they necessarily. The intelligence community must communicate specifics to institutions as early as possible. It is important to find out if newly imposed requirements are having the desired effect before additional requirements are imposed, and whether the problems being identified are new behaviors or a new discovery of old behaviors. The need for consistent requirements is common in every discussion on the issue. Consistency and simplicity are critical to avoid confusion and to facilitate compliance.

Due process is a concern. The process for some security-related cases and the approach to the consequences have been opaque to the academic community. In contrast, policies for serious issues like research misconduct and sexual harassment are generally fair and predictable for the institution and the researchers involved, especially for those who are innocent or had innocuous infractions. Policies related to research security also must be consistent and predictable.

---

colleges, universities, and laboratories." It states, "to the maximum extent possible, the products of fundamental research remain unrestricted." See https://irp.fas.org/offdocs/nsdd/nsdd-189.htm.

[7] Streitz referred to two COGR publications: 1) Framework for Review of Individual Global Engagements in Academic Research, available at https://www.cogr.edu/sites/default/files/COGR%20Framework%20Formatted%2001142020.pdf; and 2) Principles for Evaluating Conflicts of Commitment Concerns in Academic Research, available at https://www.cogr.edu/sites/default/files/Final%20for%20publication%20COC%20Principles%20Document%20V%202%20Sept%2021%202021.pdf.

Senior leadership at large institutions recognize there is an issue and have productive relationships with FBI field offices, but the leadership of small and mid-sized institutions may not have such relationships. It is also true that, in academia, faculty are fiercely independent and do not always respond to being told what to do. It is important for faculty to understand that, while a tiny minority have been prosecuted for breaching security, the problem is more widespread. The need for transparency is not unreasonable. Fear and mistrust is large, including among ethnic communities who feel they are being targeted.

Streitz suggested that the best way to start to build trust and communicate is with faculty leadership—the faculty senate, deans, and department chairs. It is important to take care to be apolitical and provide faculty as much information as possible. Scientists need hard data to bring them around.

The situation is evolving and will hit a steady state. What will it look like? What will be the balance? What type of research security oversight does fundamental research need? The next steps should be based on where we are *now*, not where we were, which may need an assessment. Due process must be normalized, and the costs must be considered.

Sarah Spreitzer

Spreitzer reflected on ACE work with its membership and with national security agencies.

In looking at the risks and benefits of U.S.-sponsored research, policy makers seem to forget about the benefits of open research and international collaboration. Rather than just talk about the risks, a risk-benefit analysis is needed. Faculty point to competing policies related to national security and open research: they are supposed to share their research but also protect it. Efforts have been made to standardize requirements at the federal level, but several new legislative proposals may complicate them. Overlapping reporting requirements and creation of burdensome regulations can slow down or block research and particularly discourage younger researchers.

There is widespread support for foreign engagement and access to foreign STEM talent, including for international students and research partnerships. Spreitzer asked: If Congress is unable to act, what can be accomplished on the regulatory side? The White House has made

changes to expand the number of STEM fields eligible for Optional Practical Training and has sent a more welcoming message to prospective students. Processing times and the overall visa process continue to be frustrating for international students and scholars. Meanwhile, competitive nations, such as Canada and the United Kingdom, are expanding pathways for post-graduate work.

Spreitzer called attention to the "foreign malign influence" on international students, in which their home governments monitor them or pressure them to speak out or be silent on campus. Much has been done to coordinate with organizations in other countries on research security, but governments have different policy ideas about how to address it. More needs to be done to align policy discussions to facilitate partnerships and exchanges with allies.

While the implementation of NSPM-33 is moving ahead, Spreitzer said that what is working now (and what will not be working in 5 or 10 years) is unclear. What will be the positive or negative impacts, she asked. National security agencies are communicating with higher education, but more can be done. Agencies should be aware of what each is communicating to the academic community. Recognizing the need for transparency, the question is how to address security issues more broadly.

The Roundtable could discuss how to build relationships with faculty and professional societies post-China Initiative anew. Many faculty felt they were unfairly targeted, and some institutions were encouraged to take actions against faculty who were not convicted. The federal government needs to rebuild trust. The current message about a shift to institutional, not individual, compliance has not been heard.

Discussion

Costs: Streitz said COGR is starting to compile data on the costs of complying with new research security requirements, but its members are large institutions. Anecdotally, some smaller institutions are wondering whether they can take on federal work because of the cost of compliance. Spreitzer said that to comply with Section 117 of the Higher Education Act (which relates to foreign gift reporting), large institutions have spent millions of dollars. Some have said it is not worth doing partnerships under the requirements of Section 124, a proposed new section to the Higher Education Act that would require extensive reporting on foreign gifts of *any* size.

Foreign Students and International Partners: Roundtable members expressed concerns, beyond concerns about the over decline in numbers of international students, about whether the United States is becoming the second or third choice for the best students. According to Mester, the National Bureau of Economic Research (NEBR) has performed preliminary research that indicates that domestic students, especially among underrepresented communities, perform better when surrounded by immigrant students. Spreitzer mentioned a working group that brought countries to the table to develop the G7 Research Compact, which seeks to identify common threats and best practices for international collaboration. She said other countries are trying to get a handle on the concept of "foreign malign influence" and the extent to which countries may be targeting or watching their students abroad. She pointed to Australia as a country that has been following this issue closely.

Intelligence Community–University Relations: Beyond individual productive relationships in specific FBI field offices, Streitz said the Office of Private Sector at FBI headquarters has sent the message to all field offices about the need for productive relationships with universities. It is a slow process to change culture, but it is happening. A Roundtable member noted faculty are independent. Companies may be told they are responsible for the actions of their employees, but it is complicated for a university, given the penchant for faculty independence, he commented. Spreitzer observed that having NSF and NIH in the room when the FBI is discussing security concerns is more valid for some faculty members.

Risks and Benefits: More broadly, is the biggest threat that research is leaking or that U.S. research is suffering a decline in output? The presenters urged that we should be looking at the benefits of open science, not just the risks. To Streitz, the principles behind NSDD-189 are sound, in which fundamental research is open and shared. She urged "high fences around small yards" in order to advance science to the greatest extent possible.

Clarity and Consistency: Researchers and institutions want clarity. While real-world examples are helpful, it was stressed that examples from a few years ago, before new protections were in place and awareness raised, are not useful. There needs to be a way to show the concern without

setting off alarm bells. Streitz commented that the community is waiting for forms and other materials from the White House Office of Science and Technology Policy (OSTP) to fully implement NSPM-33. The message about NSPM-33 is out to larger institutions, but an open question relates to what less research-intensive and smaller institutions understand and can implement.

INTEGRATING U.S. GOVERNMENT, PRIVATE SECTOR, AND SCIENCE-SECURITY EXPERIENCE: LESSONS FROM THE BROADER RESEARCH EXPERIENCE

Roundtable co-chair **John Gannon** (National Security Council, retired) moderated the panel, which consisted of **Ann Campbell** (Sandia National Laboratories), **Teresa Smetzer** (Smetzer Associates, Inc.), and **Dawn Meyerriecks** (MITRE). In introducing the session, Gannon noted an imperative for a whole-of-government approach to address the current complex threat environment. He asked the speakers to consider the same topics as the previous panel: (1) promoting and protecting U.S.-sponsored scientific research as a national security asset; (2) foreign engagement and access to foreign STEM talent; (3) accessing current and reliable relationships between scientists and security professionals; and (4) establishing relationships between scientists and security professionals.

Ann Campbell

Campbell reflected that, as a graduate student and early in her career at Sandia National Laboratories doing basic research, she did not think of the need to protect her work; the focus was on publishing and being visible. She spent her early career on Department of Energy-sponsored basic research.

Campbell established constructive relationships between scientists and security professionals. One of the keys in her move from a “blue sky research” approach to a more cautious national security perspective was working with mentors who understood how to balance the risks with the benefits and to structure programs to bring in unclassified research as an element of sensitive/classified programs. It is important to include the security professionals as

early in the project as possible. It is important to know how to parse a particular project to bring in uncleared researchers, including foreign nationals, as needed to accomplish the mission. A range of security professionals assisted. The key was to build trust with those partners.

Campbell asked two questions: "Why is the research important?" and "Why are concerns about threats important?" The key is to develop a plan moving forward and focus on the security infrastructure. A program leader may need to bring the researchers along. It will not always be obvious to them why there are some constraints and why some pieces of research may not end up being published. The converse side is to support an open research community, which must also become part of the security plan. Threat awareness enables this in a smart way.

It costs money, but mainly time and energy, to build relationships and understand perspectives. Ultimately, making that investment clarifies what needs to be done. In reality, many of the technologies are dual use. Security partners can provide helpful information, including about international travel, to keep researchers and their information safe.

A tight relationship between a security organization and government sponsor boosts the credibility of the program and allows the sponsor to have more confidence in the research program. E. Bruce Held, who formerly led Sandia's counterintelligence program, established a successful model for a counterintelligence program to understand foreign threats and educate scientists and researchers. His approach has been a great model for building a culture of trust. The team he put together included those with experience in government and the law enforcement community (including the Federal Bureau of Investigation) to provide the CI context and technical savvy to understand the issues involved in a particular research endeavor.

The relationship between researchers and security professionals is critical and most effective when based upon mutual respect and trust. What is important is spending the time to describe the research being done and why and for security professionals to understand technical details at a high level. This gives them a sense of ownership and excitement about the mission. Investment is needed up front, it is a modest cost that yields major benefits. In Campbell's experience, the research can be carried out with effective security.

Teresa Smetzer

Smetzer gained practical experience as an S&T analyst early in her career at the Central Intelligence Agency (CIA) and has been an innovator since then, leading initiatives that involve intelligence, academia, and industry. There is an enormous mandate to accelerate and pursue engagement because security challenges have never been more daunting. There is a need to balance individual organizational imperatives while cooperating and addressing challenges in a secure way. There is a need to systematically inform the private sector and academia of foreign threats and offer suggestions on strategies and best practices. She related an observation expressed by a colleague about the need to shift thinking from risk avoidance to risk management to risk mastery.

Mechanisms should be established to share information across organizations to understand mission imperatives and points of view and to share best practices on things that have been particularly effective in strengthening national security and academic excellence. She shared a number of examples that she has seen in her experience. Georgia Tech Research Institute (GTRI), for example, has provided a tremendous benefit to the government but has also benefited Georgia Tech. GTRI has been able to isolate sensitive work while also bringing in Georgia Tech researchers without security clearances when needed. Efforts to exchange staff across the elements of the ecosystem are helpful. For example, University of Texas (UT) hired a former CIA official to lead its intelligence studies program. This individual has also been an advocate across the university and has sensitized others to opportunities and threats. The CIA Digital Futures Program, which she used to direct, created detailed use cases based on real-world intelligence challenges.[8] It took a lot of work to provide sufficient detail without including classified information. Sessions were held with academia, industry, foreign partners, and the domestic government sector in the same room to brainstorm and identify best practices. Participants formed relationships and networks, and the organizations involved had a better understanding of each other.

The Center for Identity at UT spans several departments, e.g., law, engineering, business.. Wright State University had a University-Affiliated Research Center Laboratory (UARC) that was spun out as a 501(c)3. It has been enormously successful because it can move at the speed of a company. The UARC collaborates with Wright State, includes foreign faculty and students,

[8] The Digital Futures Program is within the CIA Directorate of Digital Innovation. For more information, see https://www.cia.gov/about/organization/.

and generates revenue. Utah State University's UARC hired CIA and National Security Agency retirees to expand the program. These individuals made a huge difference by bringing in government research dollars, students from other parts of the university, all while operating in a remote rural location. Smetzer said that academics also come into intelligence agencies on short-term assignments, but suggested that a more systematic approach for doing this would be useful. Federal agency staff detailed to universities are also beneficial.

Top-down mandates are hard and collaborative approaches are more useful. Such approaches are hard to codify, and this will be an ongoing challenge as new technologies and problems emerge.

Dawn Meyerriecks

In her previous position as deputy director of S&T at CIA, Meyerriecks reviewed physical, human, and supply chain attack vectors. Such reviews have become more complicated today because of the sophisticated application of at least two of those vectors to get to the end game. "Small yards, big fences" is a good goal, but these "yards" are often gated in ways we do not understand. Sophisticated adversaries take advantage of, for example, a person and a cyberattack; previously, they may have thought of those vectors separately.

It is important "not to deliberate to death." Those who have invented a technology have the best perspective on how to protect it. Meyerriecks supports involving engineers early in the process to consider how to enhance the security of the specific technologies they develop.

NSPM-33 was a good first starting point, but it is important not to just check the boxes and say we are done. We are all sinks and sources and need to avoid a checklist mentality.

Great partnerships can happen with international partners. At the CIA, Meyerriecks looked at the academic reputations of universities in partner countries, such as close European partners and the Five Eyes, to identify which would be expert on behalf of the intelligence community on a particular topic. From an S&T perspective, there is more work than talented people to perform it. While a fan of working with institutions in foreign countries, Meyerriecks noted that we are beholden on how well the other countries educate academics on security matters.

Many universities have centers sponsored by industrial giants. Industry can be a source of knowledge and experience about current and emerging threats. For example, companies are very aware of the threat of working in the media environment in Russia, Apple is an expert in supply chain management, and the Big Four tech companies (Apple, Amazon, Meta/Facebook, and Alphabet/Google) are very involved in cyber threats. Industry is not just a source of problems and funding, but can provide expertise the threats that they are seeing.

Appropriate local control and autonomy are important. Inventors are in a better position, for example, to introduce identifiers that would make technology attributable. Real technologists—not those removed from the day-to-day work with the technology—are needed to make recommendations that can protect the research community. COGR and ACE are great examples. The academic community can create communities of practice to develop their own response.

Discussion

Innovating in the 21st Century: In response to Roundtable questions about whether the security community understands emerging technology and the speed of innovation, Smetzer acknowledged that there are many regulations and restrictions, but that institutions have been creative in how to comply responsibly while remaining innovative. Meyerriecks said that every security plan must be individualized and that a checklist mentality should be avoided. Campbell agreed it takes time to have the creative discussions needed to educate security professionals who have a range of technical abilities and researchers who have a range of understanding about security vulnerabilities. It is hard to move from a risk conversation to an acknowledgment that the world is based on technology and speed. The United States can miss out, a Roundtable member observed. Meyerriecks pointed out the government has difficulty calculating opportunity cost.

Scalability: While institutions that are larger and better resourced have set up tailored parts of their enterprise to deal with security concerns, Roundtable members asked about those with less capacity. There may be a fork in the road where they opt not to invest. Perhaps some kind of

community resource can be organized for small and medium universities that do not have sufficient capacity.

Building Trust: The larger goal is a culture of security awareness within an open research environment so that it is understood why some things need to be protected, why openness is important, and what procedures are available. Consistency of what is asked of institutions and individuals is important for answering questions like: Where do I go if I have a question? What is the mechanism to resolve ambiguity? A Roundtable member identified three points of contact – OSTP, the National Security Council, and the Cybersecurity and Infrastructure Security Agency – within the government. Despite recommendations for a whole-of-government approach to research security, each agency will not go beyond the domain given it by Congress.

There is a need to provide guidance in an unclear world, but there may not be a set of clear written rules for every situation, especially those involving dual use. Meyerriecks said industry has been able to quickly make changes to improve security when needed without waiting on the government. Similarly, academics may, in some cases, be better positioned to develop alternate models than government staff.

CYBERSECURITY AND RESEARCH SECURITY

In introducing this session, Roundtable member **Chaouki Abdallah** noted that, while the previous sessions had already referenced cybersecurity, third session panelists had been asked to focus on: (1) cybersecurity at federally funded institutions; (2) cost of implementing federal cybersecurity requirements; (3) adequacy of local IT support infrastructure and software to address threats; (4) accessibility of the Office of the National Cybersecurity Director to universities; (5) effect of proliferation of CUI (controlled unclassified information) and associated cybersecurity requirements on the research environment.

Session panelists were **Brandon Wales** (Cybersecurity and Infrastructure Security Agency [CISA]), **Krysten Stevens** (Research & Education Networks-Information Sharing & Analysis Center [REN-ISAC]), **Craig Partridge** (Colorado State University [CSU]), and **Fred Cate** (Indiana University [IU]).

Brandon Wales

Cyber threats are proliferating faster than our ability to deal with them. Threats are coming from nation-states and criminal organizations. Attackers aim for targets that were previously considered too big, thanks to advanced technology in ransomware. For the research community, most cyber threats will come from nation-states. During the pandemic, vaccine development was targeted. Nation-states are targeting National Labs and Federally Funded Research and Development Centers (FFRDCs). The threat environment is getting worse. So, too, is the vulnerability marketplace with the rise of zero-day marketplaces that buy and sell code vulnerabilities.[9] That said, the research community, and FFRDCs in particular, are a target but also a great source of innovative thinking and expertise on cybersecurity.

Much is involved in building the right level of cybersecurity and creating a viable funding model. In industry, cost can be passed on to customers. It is important to figure out how to provide support to small and mid-size enterprises and the research community. A lot of technology has been developed, but integrating these cybertechnology measures into existing systems is difficult for organizations that do not have dedicated personnel with the expertise to do so.

The Office of the National Cyber Director is developing a new social contract to consider emerging issues in cybersecurity. If, however, a group does not have the ability to deploy services and protections, what is the obligation of the large companies and the government to provide that support? How can the umbrella be extended into supply chains? New thinking is needed to achieve an approach that is scalable and benefits multiple environments that do not have appropriate tools and resources.

Krysten Stevens

[9] For information on the threats of zero-day vulnerability marketplaces, see N. Perlroth. 2021. The untold history of America's zero-day market. Wired, February 14, available at https://www.wired.com/story/untold-history-americas-zero-day-market/.

REN-ISAC shares threat intelligence among its members. Cybersecurity at top tier, research intensive academic institutions tends to be mature. Depending on the size and level of research involvement, cybersecurity operations are either part of a central security program or a separate program. Rules and regulations, contracts, and data use agreements with strict cybersecurity requirement challenge established research programs - and especially institutions starting research programs.

A white paper recently issued by the IU Center for Applied Cybersecurity Research found that research cyber is most successful when it reduces burden on the researcher.[10] If too cumbersome, researchers will find ways to circumvent cybersecurity measures to keep their research on schedule and on task.

REN-ISAC does not track costs, but established programs with dedicated research security protocols, cybersecurity requirements are already being met. Infrastructure varies greatly by institution and is addressed to the best of an institution's abilities. More clarity is needed around cybersecurity requirements. While some research institutions have separate security personnel, most are supported by a central team.

The effect of the proliferation of CUI and other cyber requirements on the research environment can vary. Within institutions that are already complying with an initial contract, an additional contract may not impose any significant additional requirements in order to achieve compliance. Institutions collaborating with each other may or may not need to meet certain requirements because of their role in the collaboration, e.g., when another institution takes responsibility.

Craig Partridge

Before Partridge came to CSU, he led an effort to make Raytheon Defense Federal Acquisition Regulation Supplement (DFARS)-compliant. The process, done right, was very expensive and often difficult to do in a way that allowed researchers to get their work done. About 80 percent of projects could use a standard package of tools to be CUI-compliant. The

[10] V. Welch. 2021. A Strategy for Collaboration between Information Security Education, Operations, and Research at Indiana University, available at https://hdl.handle.net/2022/26522.

remaining 20 percent had a menu of options, with some odd problem spots. Research information systems, for example, often lack access controls. They may operate with an external processor with an older version of Windows. Updating everything would involve extraordinary costs. Access to the Dark Web would be considered inappropriate from a security perspective, but it is necessary for some researchers to have access for research purposes.

For CSU, most of the NSPM-33 implementation guidance seems feasible, as long as things do not go "overboard on authentication/authorization mechanisms." There are, however, three areas of concern. The first is how to verify and control/limit connections to and use of external information systems. A researcher has no clear way to identify inappropriate use of these systems in a real research environment. Second is how to provide protection of scientific data from ransomware and other attacks through extensive back-ups. Most researchers use a RAID drive but do not back up their data because of the high costs involved. Partridge estimated that, at CSU, the amount of data not backed up on a sophisticated back-up system is up to two orders of magnitude greater than data that is backed up. A third area relates to the installation of malicious code protections at appropriate locations and scans of files from external sources. Putting malicious code extension on all external connection systems is not possible for IP reasons. Further, some faculty use their own laptops, rather than university computers, because of university IP rules.

Fred Cate

Indiana University (IU) has 1,700 employees working in IT and the institution sees both sides of the issue—as cybersecurity researchers as administrators of grants with federal cybersecurity requirements. Many new requirements have been established vis-à-vis privacy laws, European regulations, vendor agreements, etc. Regulations on data shift liability but do not enhance security or protections. Cyberattacks are a longstanding and growing threat, but Cate cautioned against seeing attacks in every corner. Most universities are seeing attacks, but these are primarily on employees, financial, and other data rather than research data, he said.

Cate is seeing an over prescription of CUI requirements to places where they are not needed. This one-size-fits-all, or "if a little is good, more must be better," approach raises real challenges, and it leads people to look for ways around them: If researchers understand why the

requirement is needed, they will follow it, if it used needlessly, they will find a way around it. If entry costs are too high, this also interferes with other priorities, such as getting smaller institutions and underrepresented populations involved in research.

Research institutions are not required to provide cybersecurity incidence reports to the federal government, but academic institutions expect such reporting will be required in the future. Federal laws often duplicate state laws—Indiana University is subject to five sets of state laws on security breaches – but a sixth set from the federal government does not seem to do anything for security. Cybersecurity regulations are essential, but implementation should be designed to have as little negative impact on research as possible.

Costs are significant. The functions of IT security, research security, and the office on foreign interference overlap. While not a big percentage of indirect costs, if the cost is not necessary—both in terms of financial costs and costs related to non-financial costs, efficiency, and impact of research – it is problematic. Beyond security, it is important to think about reliability, integrity, and accessibility so there is security that works.

Discussion

The Nature of Cyber Threats: Responding to a question about the quantity of threats, even if they are not that sophisticated, Wales responded that multiple nation-states have compromised research at multiple universities in multiple disciplines. In many cases, the attacks are not sophisticated, but adversaries make repeated attempts to compromise (and have succeeded in compromising) critical research. Cate said the data he sees shows universities are not the first place that attackers go for research data, although the situation may be different for defense and defense contractors. Stevens said the data that REN-ISAC sees leads her to conclude that attackers are mostly looking for compromised credentials to move about laterally to see what data they can find. Wales said that it is important to look at the research portfolio; materials science, for example, is a bigger target than social science research. Even with improved security, Wales said the attack surface is increasing. Countries like China, Iran, and Russia try to target at a scale that is “off the charts.” SolarWinds was a wakeup call and demonstrated the

length that, in this case, Russia will go to access data.[11] He estimated only 500 to 1,000 organizations in the United States have the level of sophistication to respond to sophisticated attacks.

Cyberhygiene: A Roundtable member asked what the subset of universities that do not conduct restricted research should think of doing differently. In addition to issues around back-ups and a strong firewall, Partridge said an issue is sharing between institutions. Upload onto GitHub, he said, and "the worst password wins."[12] DNA capture, sophisticated microscopes, and other new technologies are not bulletproof. Embarrassing vulnerabilities must be eliminated, but cyber problems will never be fully solved, Cate said. In his view, the biggest challenge to U.S. success is not sharing enough data.

Who Owns the Problem: Partridge estimated costs of well over 5 percent in indirect costs to deal with cybersecurity and related requirements. Other costs, a Roundtable member noted, relate to maintenance, education, storage, and the non-tangible costs of being distracted from other efforts or not pursuing a collaboration. In an era where the costs of research are rising, agencies are not providing an appropriate level of funding. There is attrition in U.S. competitiveness in the last 20 years, which is another huge cost. In response to the question "who owns the problem," Cate replied, "the sad answer is no one. Like any complex problems we focus on the immediate and not the big." Partridge said part of the solution are measures that are as easy as possible for individual researchers to implement, such as how they store data. He noted that the suggestion to "leverage the security experts on campus" is not the answer—"they do not want to be leveraged, they want to solve other problems." Wales said he was not aware of any programs to allocate resources to help universities that are not as sophisticated to put measures in place that meet the requirements for the acceptance of federal funds. He referred to

[11] Sensitive data was exposed when software developed by SolarWinds and used by many federal agencies and large private companies was hacked by a suspected Russian intelligence service. The breach was announced in December 2020 but the cyberattack had taken place many months before, according to press reports. See, e.g., https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html.

[12] According to its website (www.GitHub.com), GitHub is a platform to build, scale, and deliver software that has been used by more than 83 million developers and that houses more than 200 million data repositories.

the Department of Defense's cybermaturity model for contractors and a set of cyber performance goals that CISA has been working on.

Prevention and Response: While there are many difficult issues associated with cybersecurity, some are easily resolvable, e.g., by choice of passwords, dual factor authentication, and open campus networks. Difficult culture changes are required, a Roundtable member pointed out, because universities want to feel free and open. Stevens said that she is aware of incidents in which attackers manipulate (not necessarily steal) data or employ ransomware, but there has not been a lot of reporting on this.