NSF SECURE Center Research Security Briefing

Vol. 1 No. 13: September 25, 2025

The SECURE Center distributes research security briefings and timely alerts via its listserv. The Briefing provides a centralized resource for research security-related information, including new statutory and research funding agency requirements, new or updated federal and community resources, and significant news items and scholarly works. The Center will also assess and provide commentary, interpretation, or implementation considerations on new requirements, notices and resources, working with higher education associations, legal partners, or agencies as needed.

SECURE Center Updates & Resources

SECURE Center Consolidated Research Security Training Webpage and Updates

The SECURE Center has created a dedicated webpage for the consolidated research security training (RST) module. Information on the webpage has been updated to reflect current federal RST requirements and updated files and materials have been made available, including:

- An updated version of the module, condensed training module (CTM) 1.1, includes additional accessibility improvements for better compliance with Web Content Accessibility Guidelines Level AA standards.
- Changes were made to address potential completion tracking issues on interactive slides to accommodate slower server/client processing speeds for those who were experiencing challenges.
- CTM 1.1 has been made available for direct training on the website and provides a certificate of completion.
- Versions of the training with 4 and 6 customizable university-specific pages have been made available in response to stakeholder requests.

The Center will continue to update this webpage with the latest research security training requirements and resources.

Federal Agency News & Updates

Dr. Jon Lorsch Named NIH Deputy Director for Extramural Research

On September 18, 2025, Dr. Jay Bhattacharya, NIH Director, announced that Dr. Jon Lorsch has been confirmed as the NIH Deputy Director for Extramural Research (DDER). Dr. Lorsch has served in this role in an acting capacity since April 2025. He will advise the NIH Director on multiple issues related to NIH's extramural research program and administration. This office oversees NIH's research security efforts. (more)

Professional Association Resources & Meeting Reports

Federal Demonstration Project (FDP) September 2025 Meeting: Research Security Highlights

FDP Session: Federal Agency Updates

Presenters:
Stephanie vonFeck, Chief, Federal Assistance Planning Branch, Division of Grants Policy, HRSA
Priyanga Tuovinen, Senior Grants Policy Analyst, Office of Extramural Research, NIH
Mary Sladek, Senior Program Director, Science Mission Directorate, NASA

Kimberly Whittet, Senior Policy Advisor, NIFA
Laura Givens, Policy Branch Chief, Office of Grants and Financial Management, NIFA

Moderator: Michelle Bulls, Director, Office of Policy for Extramural Research Administration, NIH

National Institutes of Health (NIH)

Per NOT-OD-25-155, NIH has implemented a new application and award structure for applications requesting funding for a foreign component (FC). Competing applications with one or more FCs must submit applications to a complex mechanism notice of funding opportunity (NOFO) that supports International Project component type. Applications will be reviewed as a whole; however, Just-in-time (JIT) information will be requested separately, and separate—but linked—awards will be issued to the various components. Also see SECURE Briefing No. 12.

National Aeronautics and Space Administration (NASA)

NASA has adopted the format of the Common Forms for Biosketches and Current and Pending (other Support), which are available for download on the Agency's Grants Policy and Compliance site. For further training on NASA's use of these forms, an instructional video is available. NASA does not currently have an agreement in place to make these forms available via SciENcv.

FDP Session: Demonstration to Develop Cybersecurity Guidelines for Federal Research Security Program Requirements

On September 16, 2025, FDP held a session on a current Demonstration to Develop Cybersecurity Guidelines for Federal Research Security Program Requirements. The session was moderated by SECURE Center Senior Advisor Lisa Nichols, Executive Director of Research Security, University of Notre Dame, FDP Research Security Subcommittee Co-chair, and Cybersecurity Demonstration Lead. Speakers included:

- Sarah Stalker-Lehoux, Acting Chief of Research Security Strategy and Policy, NSF, and FDP RSS Co-chair
- Jarret Cummings, Senior Advisor, Policy and Government Relations, Educause
- Michael Corn, Former CISO, University of California San Diego, and Former Cybersecurity. Advisor for Research Infrastructure, NSF

Sarah Stalker-Lehoux provided background on cybersecurity requirements for fundamental research under the National Security Presidential Memorandum – 33 research security program (RSP) requirements, which apply to institutions receiving more than $50 million in federal awards. Per the White House Office of Science and Technology Policy July 2024 final guidelines, institutions will need to implement a cybersecurity program one year after publication of the final NIST cybersecurity resource (IR 8481: Cybersecurity for Research). The question for agencies was, what would institutions certify to?

Through an FDP demonstration, the Research Security Subcommittee, partnering with Educause, is

leading an effort to develop flexible, risk-based guidelines to address cybersecurity threats to research as part of federal RSP requirements. The guidelines are being developed collaboratively with community and federal agency partners and the engagement of knowledge experts representing a broad array of research organizations, programs, and roles.

Jarret Cummings provided an overview of what is covered in the research cybersecurity plan, including roles and responsibilities across institutional stakeholders, risk assessment (e.g., how to conduct, frequency) and mitigation. Implementation of the NSF Critical Controls Set was reviewed by Mike Corn. They include 14 basic controls such as multi-factor authentication, anti-malware, data backups, and others. Exceptions and compensating controls would be implemented as needed at the institutions' discretion. Additional information on the controls can be found here.

The working group anticipates sharing the draft guidelines with the broader FDP community later this month and providing the opportunity for feedback. The intent is to deliver the final guidelines to NSF and the federal interagency in the late-November/early-December timeframe.

FDP Session: Expanded Clearinghouse Subcommittee - Research Security & Subawards

Presenters:
Amanda Hamaker, Purdue University
Robert Prentiss, Yale University
Jennifer Rodis, University of Wisconsin-Madison
Taren Ellis Langford, University of Arizona
Jennifer Ford, University of California San Diego

The Expanded Clearing House (ECH) Subcommittee presented an overview on the purpose of the ECH (to reduce burden for commonly shared institutional data) as well as recent updates for the fdpclearinghouse.org institutional profiles. They noted there are currently 376 profiles in the database: 216 FDP members and 159 non-members (whose participation is fee-based). As context for the discussion, the Subcommittee presented background on:

- National Security Presidential Memorandum - 33
- Research Security Program requirements (noting the pending federal guidance on three of four areas: cybersecurity, foreign travel, and export control)
- The malign foreign talent recruitment program (MFTRP) prohibition in the CHIPS and Science Act of 2022
- A summary of the NSF SECURE Center

The ECH Subcommittee described its activities and its overlap with the Subawards Committee and the Subawards Committee's standardization initiatives for FDP membership.

Introductions were made to the 15 members of the Research Security & Subawards Working Group, co-chaired by Taren Ellis Langford, University of Arizona and Jennifer Ford, University of California San Diego. The purpose of the Working Group is to review the intersection of research security with ECH's areas, partnering with the Subawards and Research Security committees as needed. Initial focus

areas for this group include current requirements, a sustainable approach, the changing landscape, and identification of covered institutions.

The group presented on its goal to implement a new field in the ECH institutional profile to indicate NSPM-33 "covered institutions." Implementation is planned for January 2026. Discussion included possible identification of these institutions using the three-year average in the NSF Survey of Federal Science and Engineering Support to Universities, Colleges, and Nonprofit Institutions 2023 and pre-population by the FDP into existing ECH profiles. Many audience members agreed that this would be beneficial and reduce administrative burden, rather than having each institution populate the field. Attendees raised additional questions, including how to certify research security training for individuals, and concerns about smaller subawardees providing certification. A suggestion was made to revise the Letter of Intent (LOI) template to include text about research security and the MFTRP prohibition. The Committee chairs noted that, due to the variety of stakeholders involved in the LOI template review process, changes to the LOI template could take about a year and these suggestions were tabled for further consideration and possible updates at the January FDP meeting.

FDP Session: Recent Insights from NSF's GRANTED Program September 2025

Moderator/Hosts:
Susan Anderson, ERI Committee Co-Chair, College of Charleston
Dina Stroud, Program Director, Growing Research Access for Nationally Transformative Economic Development, National Science Foundation (NSF)

This session consisted of presentations from two GRANTED Project Teams:

- RISC and GRANTs Made: University of Maryland-Baltimore County (UMBC) Scholarly Impact
- Filling the Gap: University of South Alabama

Dina Stroud, NSF Program Director, began the session with an overview of the research enterprise, challenges faced, and where the GRANTED Program seeks to fill those gaps. The GRANTED Program provides funding opportunities for ideas that will: generate scalable models of sustainable capacity; create new collaborations and communities; increase the range of leadership and institutions funded; and strengthen engagement across the research enterprise. These funding opportunities are ongoing. Proposals should directly relate to the research support and service infrastructure ecosystem. The GRANTED themes and program descriptions were presented as well as an overview of past awards. Engagement with NSF staff during their office hours, to discuss potential proposal submissions, is strongly encouraged.

The University of Maryland-Baltimore County (UMBC) leadership team of Karl Steiner, Vice President for Research and Creative Achievement, and Christine Mallinson, Assistant Vice President for Research and Scholarly Impact, presented a summary of their grant, *Building Capacity to Manage RISC: Investing in Research Integrity, Security and Compliance at UMBC through Practices, Processes & Partnerships*. The goal of the project is to build scalable knowledge for research security infrastructure, which started at their own institution, including the development of materials and an institutional self-assessment to identify gaps. The extension of their partnership work with the

University of Maryland Eastern Shore, Delaware State University, and Morgan State University was highlighted. As part of their current year of funding they are conducting a survey to understand how institutions are addressing the evolving research security requirements. They invite compliance professionals from other institutions to visit their website to complete a brief survey.

The UMBC team also presented their work on *GRANTS MADE at Scale: Implementing a Regional Research Administration Student Internship Program in Maryland and Delaware* which create opportunities at several partnering institutions resulting in 52 interns trained by 2029 in research administration (one dedicated to research security), and where the interns will be connected with the NCURA Region 2 professional community in the course of their professional development.

Filling the Gap: Establishing an Undergraduate Program in Research Administration and Grant Management was presented by the team from the University of South Alabama (USA): Lynne Chronister, former Vice President for Research (retired), Project Director; Keone Fuqua, Program Manager Curriculum Design; and overall project leadership from Chris Brown, Vice President of Research at University of Alabama Birmingham (UAB). The program is designed to prepare the next generation of research administration professionals through the creation of an academic curriculum in research administration that forms the basis for a minor, concentration, or certificate, in conjunction with an undergraduate degree. A Research Administration and Management (RAM) curriculum has been developed and launched. Several key collaborators/ subawardees are assisting in development and/or assessment of the curriculum. At the time of the presentation, the University of Southern Alabama had accepted 19 out of its 25 anticipated partner institutions to implement the RAM curriculum at their institutions. To ensure content consistency and sustainability, the Society of Research Administrators International (SRAI) hosts the modules and then provides the technical files for incorporation into each institution's learning management system. The team noted that, after the grant period, SRAI will own and maintain the curriculum. For implementation, the team profiled some of the challenges to be addressed by each institution, including an institutional approval process, faculty credentials, state level approvals (if needed), and accrediting bodies. The University of Alabama Birmingham successfully launched the initial program for Fall Semester 2025 with 20 students in the cohort.

FDP Session: Federal Research Security Panel

On Wednesday, September 17, 2025, the FDP Federal Research Security (RS) session was moderated by SECURE Center Senior Advisors Jim Luther, Yale University, and Lisa Nichols, University of Notre Dame. Speakers included:

- Michelle Bulls, Director, Office of Policy for Extramural Research Administration, NIH, and Lead FDP Federal Representative
- Steve Ellis, Program Officer, Office of the Chief of Research Security Strategy and Policy, NSF
- Jeannette Singsen, Senior Advisor, Office of Research, Technology, and Economic Security, DOE

The session covered the latest updates from federal partners on RS topics of interest, including the implementation of the Research Security Program (RSP) standards, updates on agency- specific

activities, and other topics.

National Institutes of Health (NIH)

Common Forms

NIH has launched preview versions of the Common Forms within SciENcv (Science Experts Network Curriculum Vitae). These are not the final official versions. The goal is to allow users to preview the new functionality and instructions. NIH will issue a subsequent Guide Notice announcing the final versions once clearance is obtained from the Office of Information and Regulatory Affairs. That "uber" notice will include a great deal of information.

Training on Disclosure

Michelle Bulls provided further clarity regarding NOT-OD-25-133, *New Policy Requirement to Train Senior/Key Personnel on Other Support Disclosure Requirements*. Per the notice and presentation, institutions' internal controls (e.g., policies and procedures) for Other Support disclosure must include training for senior/key personnel on these policies and procedures. Although the notice does not relate to research security programs and is applicable to all NIH recipient institutions, NIH noted that NSF's research security training modules, the Secure Center's condensed training module (CTM) (endorsed by NIH and other agencies), or an institution's own training that meets the CHIPS Act and notice requirements can be used for Other Support disclosure training. The SECURE Center notes that additional blank slides have been made available at the end of the CTM (2, 4, or 6 slides) for institutions to include their specific policies, guidance, procedures, contacts and other relevant information. All are available on the SECURE Center's CTM webpage. Per Michelle Bulls, effective October 1, 2025, training on Other Support must be taken by all senior/key personnel at the time of research performance progress report (RPPR) or just in time (JIT) submissions.

Research Security Program Policy

The NIH presentation included the September 11, 2025, notice NOT-OD-25-154, *Implementation of NIH Research Security Policies*. NIH clarified that the agency is participating in a Memorandum of Agreement with NSF and other federal research funding agencies to develop a centralized process for recipients to certify compliance with the yet-to-be-published RSP requirements. NIH will issue more information on the central certification process and timing as it becomes available.

Effective January 25, 2026, NIH will require that institutions and senior personnel submitting applications for NIH funding certify that Research Security (RS) training has been completed within the previous 12 months. There was discussion during the session that the RS training and the malign foreign talent recruitment program requirements are not just part of the RS Program requirements but, separately, a requirement of the CHIPS and Science Act. Therefore, both requirements and certifications are applicable to all applicants or recipients of federal science and engineering awards, regardless of whether institutions meet the $50 million threshold for the RSP requirements, including subrecipients.

National Science Foundation (NSF)

Steve Ellis of NSF noted the agency's planned October 10, 2025 implementation of mandatory RS training and that, per NSF's Important Notice 149, NSF, NIH, DOE, and DoD recognize the SECURE Center's one-hour CTM as meeting the agencies' RS training requirements. USDA has also indicated the CTM will meet their requirements. Steve noted that while the four longer RS training modules currently remain on the NSF website, these modules will not be updated and recipients are encouraged to use the SECURE Center's CTM. NSF also noted its Annual Certification Requirement Regarding Prohibition on Participation in Malign Foreign Talent Recruitment Programs is now In effect.

Department of Energy (DOE)

Jeannette Singsen indicated that DOE anticipates implementing the Common Forms for Biosketches, Current and Pending (Other) Support and via SciENcv in October for all Notices of Funding Opportunities (NOFOs) and awards. There will also be a supplemental disclosure form for a subset of projects that will be built into SciENcv as well. Applicability for the supplemental disclosure form is based on the sensitivity of the technology. The supplemental disclosure focuses on foreign country of concern (FCOC) connections, with questions related to past FCOC support; past FCOC incentives, past collaborations at FCOC sites (excluding routine workshops or conferences hosted in FCOCs), patent applications filed in an FCOC without a companion US patent application, and FCOC military or intelligence service. If required, it will be indicated in the NOFO. Jeannette suggested DOE is taking a risk-based approach in terms of whether Current and Pending (Other) Support, the supplemental disclosure, and/or the transparency of foreign relations form are required.

Covered individuals (Senior/Key Personnel) will need to certify that they have taken RS training within the last 12 months and that they are not currently participating in a malign foreign talent recruitment program. New covered individuals added to the project after award/selection are required to certify they have taken the RS training within 30 days of joining the project. As indicated by other agencies, institutions can use their own RS training provided it meets the requirements in the CHIPS Act. There was discussion about whether other agencies would require the RS training annually, as NIH has stated. Jeannette indicated that it was likely, though not yet established, that the RS training would be required annually in association with Research Security Programs, but not for institutions with less than $50 million in federal science and engineering funding.

Regarding transparency of foreign connections (TFC), DOE has a new suggested (but optional) template which the agency indicates can make it easier to disclose. The template can be found here. Per the DOE presentation, updated TFCs must be submitted if information changes. For some awards, an updated TFC will be required as part of the continuation application.
Per statute, DOE continues to have a prohibition on individuals or entities on the 1260H or Commerce BIS Entity lists from participating on DOE proposals and awards. DOE recipients are encouraged to do due diligence to ensure collaborators are not on these lists. More information on DOE requirements and FAQs can be found on the DOE's RTES website.

FDP Session: Simplifying Research Regulations and Policies: Optimizing American Science

The FDP September 15-17, 2025, meeting included a briefing of the recently released National

Academies report, *Simplifying Research Regulations and Policies: Optimizing American Science* which presents options for federal actions to improve regulatory efficiency affecting researchers and their institutions. Alex Helman, Study Director, National Academies of Sciences, Engineering, and Medicine, served as the moderator. Speakers included committee members Lisa Nichols, University of Notre Dame, Stacy Pritt, Texas A&M University System, and Christopher Viggiani, Oregon State University.

The session provided an overview of past efforts to reform research regulations and policies, and cross-cutting principles, including harmonizing agency requirements, tiering them to risk, and using technology to simplify compliance. Several overarching options were presented to facilitate reform, including:

- Establishing a permanent function within the Office of Management and Budget, an *Assistant Director for Institutional Research Coordination and Community Engagement*, with the authority to coordinate cross-agency requirements
- Appointing a Federal Research Policy Board as previously authorized in the 21st Century Cures Act
- Using FDP to explore innovative ideas and practices through pilot programs. As agencies develop new models and innovative approaches, they could work directly with FDP to test and refine them before formal launch.

The report includes options covering a broad array of research administration and compliance areas. The FDP session covered recommendations on grant proposals and management, including: introducing a federal-wide, two-stage pre-award (letter-of-intent) process; eliminating expectations for filing financial disclosure statements at every transaction; and a centralized financial disclosure system. In the area of conflict of interest, creating a uniform federal FCOI in research policy or reverting to the previous $10,000 Public Health Services threshold.

In the area of protecting research assets, Federal-wide implementation of the NSPM-33 common disclosure forms and pre- and post-award table without deviation as the primary means to identify conflicts of commitment; using the SECURE Center as an interactive research security information hub; renewing the Export Control Reform Initiative with input from academia; and, adopting a risk-tiered approach to export controls.

The report explores ways to streamline research misconduct proceedings including the creation of a single, flexible federal misconduct policy to which all funding agencies defer, or the option to more clearly designate a lead agency to coordinate cases involving multiple funders.

The report also highlights the complexity of regulations governing research with biological agents and toxins. Leveraging successful oversight frameworks, it provides options for a more centralized, coordinated federal approach to biosafety oversight, through a single agency that registers and empowers institutional biosafety committees. The report also offers an alternative that would shift responsibility for identifying DURC and gain-of-function research to federal funders.

The session highlighted several options provided in the report to enable the USDA and NIH Office of Laboratory Animal Welfare (OLAW) to harmonize, streamline, and modernize their oversight

processes, including for NIH OLAW to adopt an online platform and streamlined approach for its Animal Welfare Assurance process.

The options presented aim to improve regulatory administrative processes and modify or eliminate policies and regulations that have outlived their purpose while maintaining necessary and appropriate integrity, accountability, and oversight.

FDP Session: The SECURE Center -- Solutions and Initiatives to Empower the Research Security Community

Moderator/Host: Steve Post, University of Arkansas for Medical Sciences

Speakers:
Mark Haselkorn, University of Washington
Sonia Savelli, University of Washington
Robert Nobles, Emory University
Lee Stadler, University of Missouri Kansas City

Sonia Savelli, SECURE Center Creation Director, led a demonstration of the SECURE Center's Shared Virtual Environment (SVE) and various research security resources related to foreign travel and travel-sensitive topics, including: Basic and High-Risk Travel Checklists, A Travel Resource Guide, and a Sample Travel Briefing to support the activities of both researchers and research security professionals.

On September 15, 2025, the SVE had its initial release for testing, marking the beginning of a Use Feedback Refine (UFR) process. UFR is an iterative approach designed to gather user insights that guide the development and refinement of the SVE. During the first week, 27 users, who are designated Research Security Officers for their institutions, participated in guided sessions to provide feedback on the SVE and its products. Their input is helping the SECURE Center Co-Creation teams refine the SVE ahead of broader release and onboarding. The UFR process will continue even after the SVE is broadly released to ensure continued relevance and user-friendly functions.

Following the presentation, discussion ensued with SECURE Center members, regarding the features demoed in the SVE and particularly when the system would be available. As the UFR process has started, several items needing resolution have been identified. Once items are successfully resolved, the SVE will be opened to interested users.

Questions were also raised about the availability of the web-based Consolidated Training Module for RS training. The SECURE Center webpage and materials have been updated. It was noted that a certificate of completion can now be downloaded on successful completion of the training.

As shared during the session, the capabilities of the SVE will continue to expand over time, providing resources that bolster the research ecosystem through the shared perspectives of a wide stakeholder base. Engagements between the FDP and the SECURE Center have become a vital channel of contribution to understanding the multi-faceted nature of research security.

U.S. Congressional Activity

House Republicans Express Concern Over Theft of Research Information

On September 18, 2025, U.S. House of Representatives Science, Space, and Technology Committee Chair Brian Babin (R-TX) and Investigations and Oversight Subcommittee Chair Rich McCormick (R-GA) sent a letter to MD Anderson Cancer Center expressing concern regarding a July 9, 2025 security incident involving an MD Anderson post-doctoral researcher, charged with theft and tampering with proprietary research. (more)

Research Security News & Reports

Please note, articles linked below may require a subscription to view.
NSF SECURE Center cannot distribute copies of subscription-based articles.

Cyber threat information law hurtles toward expiration, with poor prospects for renewal (Cyberscoop, 9/22/2025)

The Cybersecurity Information Sharing Act of 2015, which allows private companies to share cyber threat data with the U.S. government, is set to expire September 30, 2025. Efforts in Congress to renew or extend the law are failing, due to political disagreements. A Senate proposal for a clean 10-year extension was blocked by Sen. Rand Paul (R-KY). Attempts to attach extensions to larger bills like the National Defense Authorization Act have also stalled. Without renewal, experts warn it could weaken cybersecurity cooperation between the private sector and government, especially during a major cyberattack. (more)

Texas HB 127 brings new research security rules to Texas (*Daily Toreador*, 9/17/2025)

Texas has passed a new state law that impacts how institutions of higher education (IHEs) manage foreign gifts and research partnerships. Among its requirements, House Bill 127 mandates the establishment of a Higher Education Security Council (comprised of research security officers from Texas universities); restricts gifts from "foreign adversaries" that can be accepted by IHEs, their employees, and student organizations; requires IHEs to conduct background screenings of non-citizen/resident applicants before offering employment in research-related positions; and requires IHEs to establish international travel approval and monitoring programs. (more)

Cybersecurity Training Programs Don't Prevent Employees from Falling for Phishing Scams (UC San Diego Today, 9/17/2025)

A major UC San Diego study involving 19,500 health employees found that common cybersecurity training methods—annual courses and embedded phishing simulations—do not significantly reduce the risk of falling for phishing scams. Employees who completed training were just as likely to click on phishing links as those who hadn't. Engagement with training was low, with most users spending less than a minute on the material or closing it immediately. Over the eight-month study, phishing susceptibility actually increased, with more than half of employees clicking on at least one phishing

link by the end. The study also revealed that some phishing emails were far more convincing than others. For example, an email claiming to update the company vacation policy had a much higher click rate than one requesting an Outlook password update. Researchers recommend shifting focus from traditional training to technical solutions like two-factor authentication and password managers that detect phishing sites. Their conclusion: current anti-phishing training programs are largely ineffective. (more)

'I have to do it': Why one of the world's most brilliant AI scientists left the US for China (*The Guardian*, 9/16/2025)

An in-depth look into the factors that contributed to Song-Chun Zhu, one of the world's foremost authorities in artificial intelligence, leaving the US after 28 years here. In August 2020, Zhu returned to China, where he now leads the Beijing Institute for General Artificial Intelligence (BigAI). (more)

Research Security-Related Events & Conferences

COGR October Meeting:

Registration is now open for COGR's October 23-24, 2025, meeting in Washington D.C. at the Washington Marriott in Georgetown. Preliminary agenda topics include:

- Simplifying Research Regulations and Policies: Optimizing American Science: A NASEM Report
- Cybersecurity & Other Research Security Implementation Updates
- Legislative Update & Outlook

Save the Date for ASCE 2026:

Mark your calendars now for the 2026 Academic Security and Counter Exploitation Program. Next year is the 10th anniversary of the largest research security conference in the world: February 24-26, 2026. (more)

Looking to participate in NSF SECURE Center co-creation activities or contribute to weekly briefings?

Sign up Here!