NSF SECURE: Supporting Research Security & International Collaboration

Lisa Nichols,
University of Michigan

Lisa Nichols, Ph.D.
Executive Director, Research Security
University of Michigan

SECURE National Center,
Office of the Director

Kevin Gamache,
Texas A&M

Kevin Gamache, Ph.D.
Associate Vice Chancellor and Chief
Research Security Officer,
Texas A & M University System

SECURE Analytics PI
SECURE Southwest Regional Center
Co-Director

Mark Haselkorn,
U. Washington

Mark Haselkorn, Ph.D.
Professor
Human Centered Design & Engineering
University of Washington

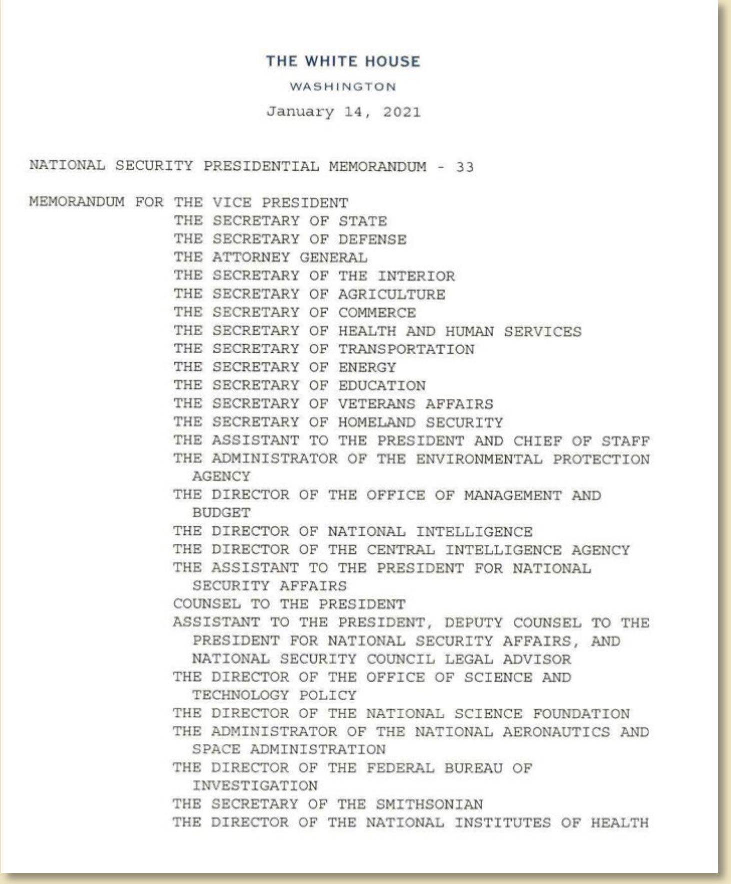
SECURE Center PI & Director

PANEL AGENDA

- Intro, background & refreshers – Lisa
- SECURE Center - Mark
- SECURE Analytics - Kevin
- Specifics, as needed – All
- Questions and discussion

Safeguarding the Entire Community in the U.S. Research Ecosystem

NSPM-33



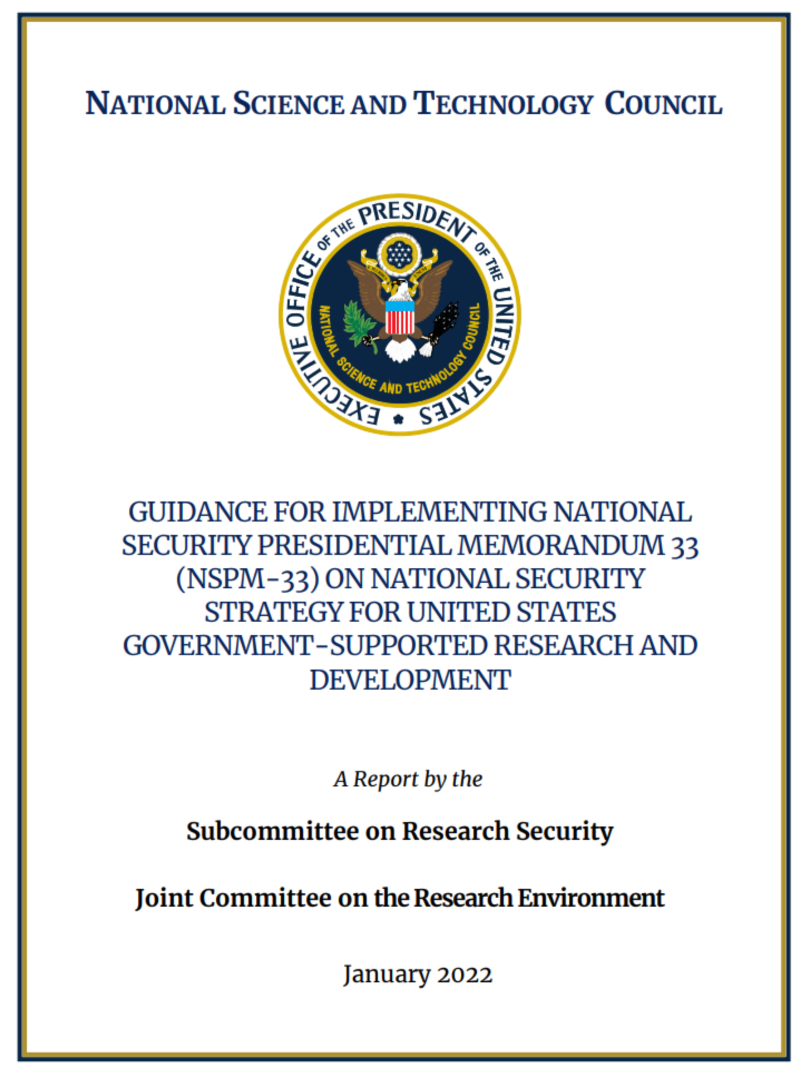
THE WHITE HOUSE

WASHINGTON

January 14, 2021

NATIONAL SECURITY PRESIDENTIAL MEMORANDUM - 33

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF THE INTERIOR
THE SECRETARY OF AGRICULTURE
THE SECRETARY OF COMMERCE
THE SECRETARY OF HEALTH AND HUMAN SERVICES
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF ENERGY
THE SECRETARY OF EDUCATION
THE SECRETARY OF VETERANS AFFAIRS
THE SECRETARY OF HOMELAND SECURITY
THE ASSISTANT TO THE PRESIDENT AND CHIEF OF STAFF
THE ADMINISTRATOR OF THE ENVIRONMENTAL PROTECTION AGENCY
THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET
THE DIRECTOR OF NATIONAL INTELLIGENCE
THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
COUNSEL TO THE PRESIDENT
ASSISTANT TO THE PRESIDENT, DEPUTY COUNSEL TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS, AND NATIONAL SECURITY COUNCIL LEGAL ADVISOR
THE DIRECTOR OF THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY
THE DIRECTOR OF THE NATIONAL SCIENCE FOUNDATION
THE ADMINISTRATOR OF THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
THE SECRETARY OF THE SMITHSONIAN
THE DIRECTOR OF THE NATIONAL INSTITUTES OF HEALTH



NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT

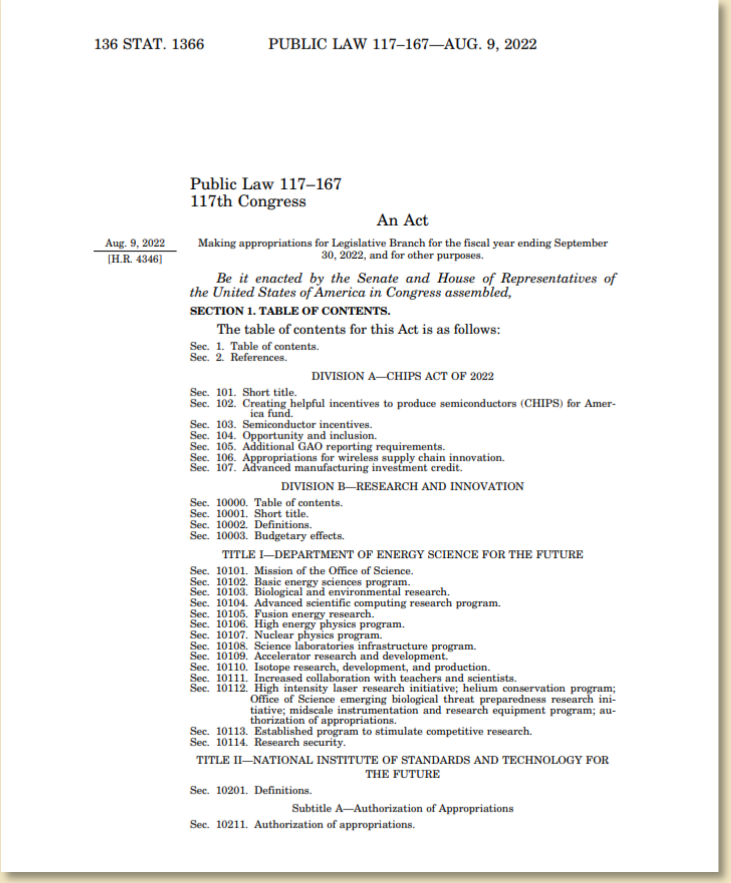
A Report by the

Subcommittee on Research Security

Joint Committee on the Research Environment

January 2022

CHIPS And Science Act



136 STAT. 1366   PUBLIC LAW 117–167—AUG. 9, 2022

Public Law 117–167
117th Congress

An Act

Aug. 9, 2022
[H.R. 4346]

Making appropriations for Legislative Branch for the fiscal year ending September 30, 2022, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

Mission:

Empower the research community to make security-informed decisions about research security concerns

Approach:

Providing information, developing tools, and providing services

Audience:

IHEs, non-profit research institutions, and small and medium-sized businesses

Duties of the RSI-ISAO under CHIPS

1 **Serve as a clearinghouse for information** to help enable the members and other entities in the research community to understand the context of their research and identify improper or illegal efforts by foreign entities to obtain research results, know how, materials, and intellectual property;

2 **Develop a standard set of frameworks and best practices**, relevant to the research community, to assess research security risks in different contexts;

3 **Share information concerning security threats** and lessons learned from protection and response efforts through forums and other forms of communication;

4 **Provide timely reports** on research security risks to provide situational awareness tailored to the research and STEM education community;

5 **Provide training and support**, including through webinars, for relevant faculty and staff employed by institutions of higher education on topics relevant to research security risks and response;

6 **Enable standardized information gathering** and data compilation, storage, and analysis for compiled incident reports;

7 **Support analysis of patterns of risk and identification** of bad actors and enhance the ability of members to prevent and respond to research security risks;

Stakeholder Desires for Functional Domains

Tools & Training

- Actionable Tools
- Frameworks
- Rubrics
- Best Practices

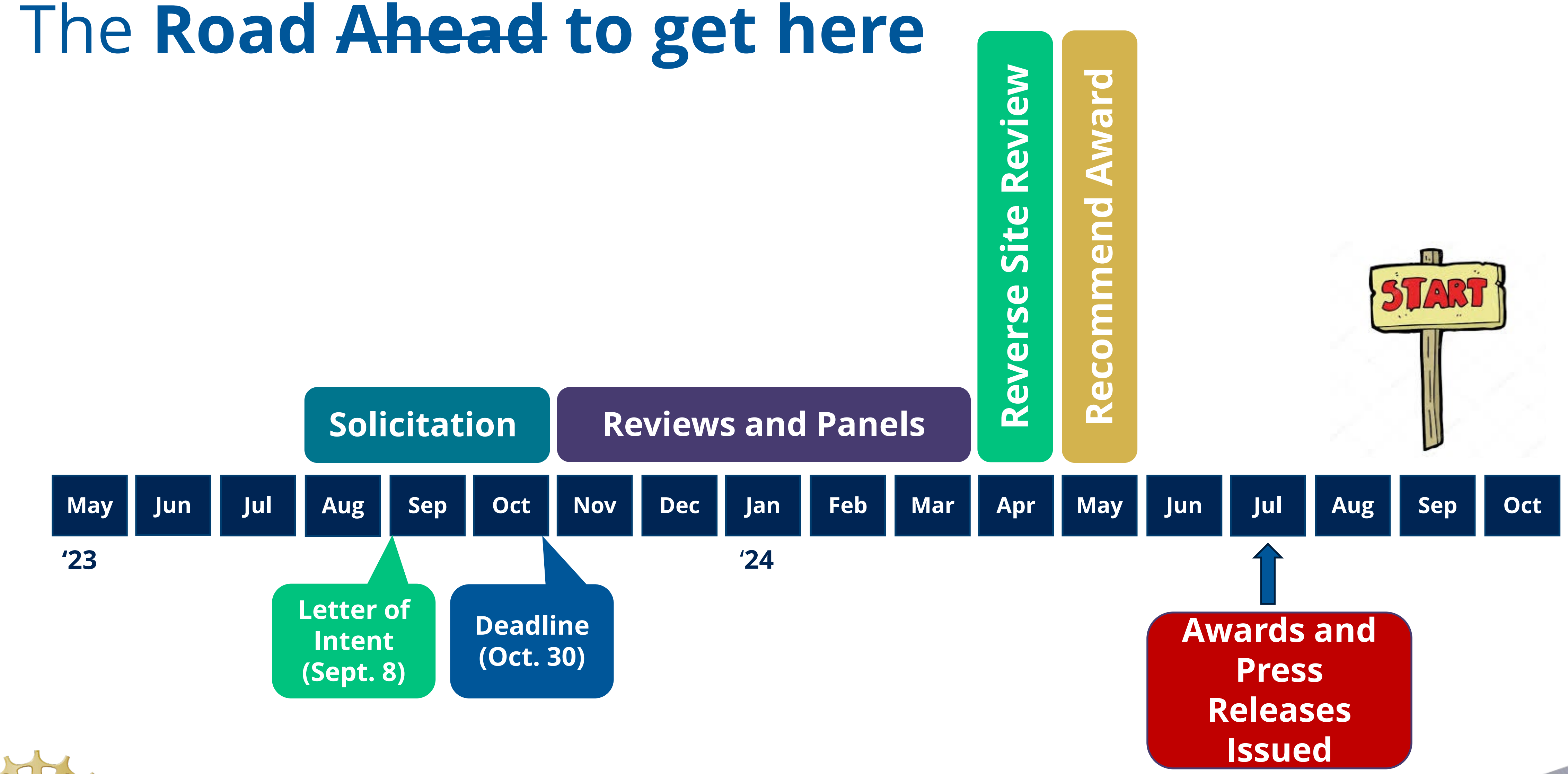
Engagement & Inquires

- Build trust
- Demonstrate value
- Reduce cost for large
- Be accessible to small

Data Analysis & Reporting

- Landscape analysis
- Risk modeling
- Timely, relevant communication

The **Road ~~Ahead~~ to get here**



Solicitation

Reviews and Panels

Reverse Site Review

Recommend Award

May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct

‘23

‘24

Letter of Intent (Sept. 8)

Deadline (Oct. 30)

Awards and Press Releases Issued

The SECURE Program

SECURE:

Safeguarding the **E**ntire **C**ommunity in the **U**.S. **R**esearch **E**cosystem

$67 Million NSF Investment

Two synergistic awards:

- The SECURE Center
- SECURE Analytics

“Entire Community”

Roles

- Researchers
- Research Administrators
  - RSOs
  - CISOs
- Funding Agency Personnel
- Others

“Entire Community”

Organization Homes

- Institutions of Higher Education (IHEs) (R1, R2, R3, ERI, MSI, HBCUs…)
- Small & medium businesses
- Non-profit research institutions
- Higher education associations and professional & scientific societies
- Others

The SECURE Center is **not** business as usual.

The Community Owns the Problems and Solutions

The research community co-designs what it wants and needs to safeguard research value at its organizations. Together we define the problems, design the solutions, and iteratively work together to make them happen and assure their use.

Administrators are Center Leadership

Administrators are SECURE Center awardees, and their knowledge of administrative processes and research security are key areas of relevant subject matter expertise. Research administrators are SMEs.

Federal Agencies will be included at the design table

In addition to guiding SECURE under the cooperative agreements and a USG Steering Committee, funding agencies will be given a place in the design process, representing their perspectives.

The award was not limited to the selected proposal

SECURE Center leaders include some from organizations that competed and early collaborators come from organizations that were not part of any center proposal.

There is a tight coupling of the two SECURE awards

The PI of SECURE Analytics (Kevin) is the Southwest Regional Center Co-Director, and the Co-PI of SECURE Analytics (Glenn Tiffert) is on the Center’s Expert Areas Team. Also, a Service Level Agreement between the two awards will be executed.

Awardees alone cannot complete the work

While a broad cross-section of the research community has been funded, we cannot accomplish our mission without the engagement of the entire U.S. research community.

Not just tools and capabilities, but a community environment

One of the things we will co-create is a shared virtual environment (SVE) that enables our trusted community to safely collaborate, deliver solutions, and share information and practices.

Our approach accommodates diversity

Capabilities and solutions provided within SVE do not have to look and work the same for everyone.

Build Together

SECURE Center empowers the research community to design, develop, implement, and maintain capabilities and solutions. Building together fosters collaborative decision-making.

National and Regional Centers

To accomplish this, we are establishing five regional centers, each with a co-creation hub: Northeast (Northeastern), Southeast (Emory), Midwest (Missouri), Southwest (UT San Antonio & Texas A&M), and West (Washington).

Other Center Components

Expert Areas: sensitive research, threat types, geopolitical and geospatial analysis, international relations (Mississippi State, Hoover/Stanford, and Michigan, to begin with)

Work with **SECURE Analytics** (Texas A&M and Hoover Institution)

Other Center Components

Value Areas: equitable access, non-R1s, underserved STEM partners, burden reduction, balancing collaboration and protection, protecting U.S. values (Michigan, College of Charleston, Washington, Hoover Institution, and MindCette to begin with)

Community at the Center

SECURE Center is more about community-centered design and co-creation than compliance.

What might we build?

SECURE Center will build what the community identifies and prioritizes. Will that include:

- Shared components of research security programs?
- Analytics for risk assessment of international collaboration?
- Iteratively enhanced training modules?
- Security alerts with useful information that doesn’t name the targeted institution?
- Malign attempts to gain information and trust?
- Pre-submission risk assessments?
- Expert advice and best practices?
- What are you thinking?

What might we build?

What we heard from a Southwest pilot last week:

Priority #1

Assessment Tools/Resources: Tools to assess international collaborations, including assessing and mitigating risky collaborations.

- Guidance, rubrics, case studies, matrices, and analytics, including “effective risk mitigation and prevention strategies.”
- Guidance for faculty on international collaborations, including the advantages and need for international collaboration and for administrators on gray areas.

Priority #2

- **Resources on Threats:** Open-source details from our federal partners regarding the threat environment. A “book of horror stories”, both involving more minor and unintentional disclosure and not. More case studies from the feds.

What might we build?

What we heard from a Southwest pilot last week:

Disclosure Resources and Tools: “AI-generated searches for consistency across publications, CVs, Other support, known lists online”

- Resources on disclosure, including evaluation
- Software for detecting undisclosed foreign agency associations

Research Security Training: Flexible/practical training modules

Resources for Navigating Federal Risk Concerns:

- Predictors and how to preempt federal risk concerns; mitigation measures; how to engage agencies; case studies on successful outcomes.

Common Practices Resources: A one-stop shop.

Resources for Preparing to Handle CUI: Workshop, training, or guidance

Processes, Forms, and Case Studies Regarding Visiting Scholars

The SECURE Center

Empowering people and organizations in the U.S. research ecosystem to better safeguard the value of their research.

SECURE Analytics Is:

A hub for data collection, analysis, and reporting to identify foreign malign behavior, share research security risk information, and improve risk assessment and training practices for the research community.

What will SECURE Analytics Do?

- SECURE Analytics will build a dedicated team of **geopolitical analysts, data engineers, and programmers** who will develop open-source datasets, methodologies, and tools to identify and analyze patterns of research security risk, threat types, and malign actors.
- SECURE Analytics will work with stakeholders, via the SECURE Center, across the research community to meet their needs, address their concerns, and enhance their capacity to detect, respond to**, and prevent improper efforts by foreign entities** to acquire research results, know-how, materials, and intellectual property.

What will SECURE Analytics deliver?

- A community-facing platform powered by extensive qualitative and quantitative datasets and accepted AI and machine learning.
    - It will empower accredited users to query the research priorities, collaboration networks, and professional associations of potential international research partners.
    - It will collect and analyze at-scale foreign industrial policies, talent and workforce development plans, and scientometric, patent, and corporate data in multiple languages;

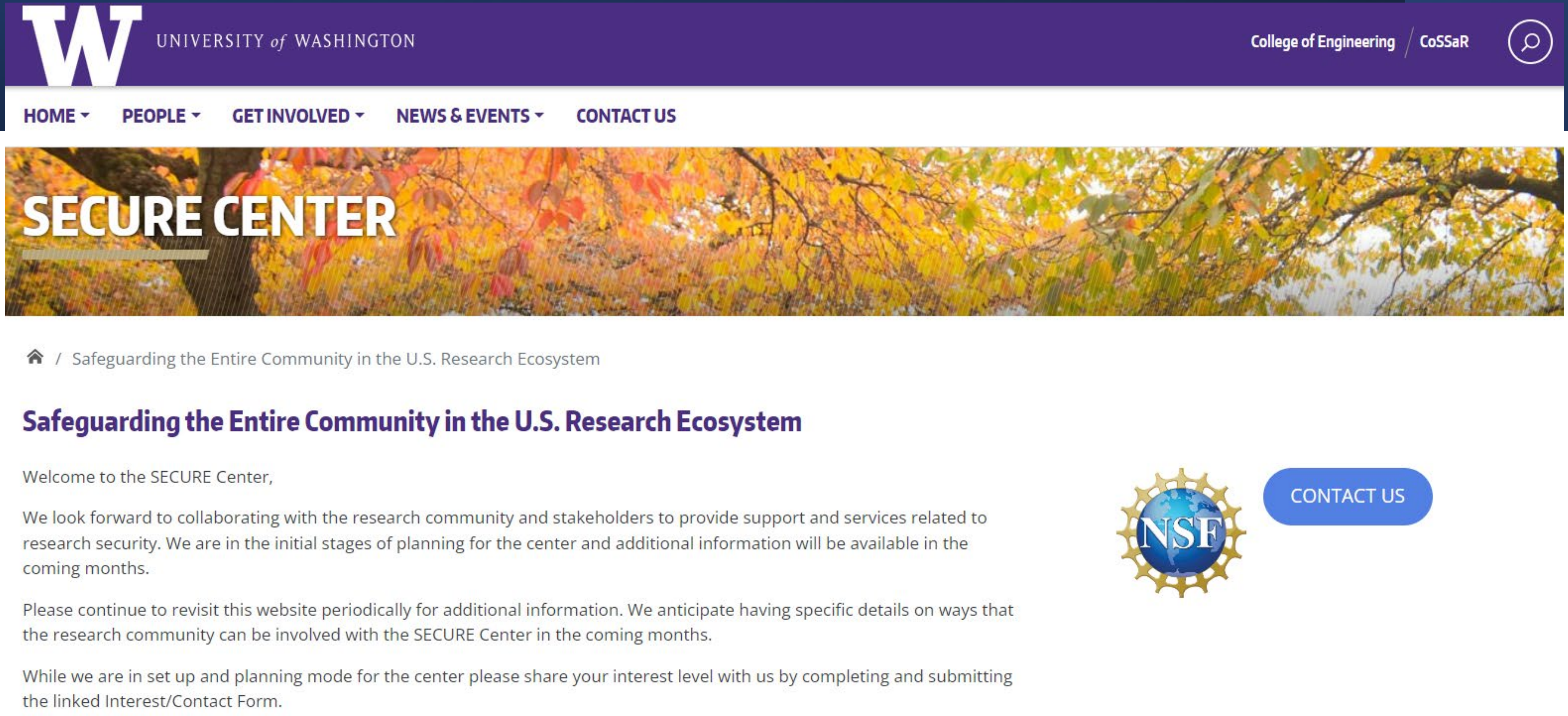
What will SECURE Analytics deliver?

- A back-end platform restricted to the SECURE Analytics team with enhanced functionality and granularity that will support incident and landscape analyses and timely reports on research security risks.
- A reference library of policies, leading practices, and research reports to raise situational awareness in the community of global research security risk in coordination with the SECURE Center
- Capacity building training on research security risk detection, assessment, and mitigation in coordination with the SECURE Center

What is the SECURE Analytics board?

- The SECURE Analytics board will counsel SECURE Analytics on its work and connect Analytics to a broader network of experts who can inform its technical assessments of foreign risk and capabilities in critical lines of research and innovation.
- The board will comprise academia, industry, and legal and national security community leaders.

Simple Initial Web Site & Interest Form



/ Safeguarding the Entire Community in the U.S. Research Ecosystem

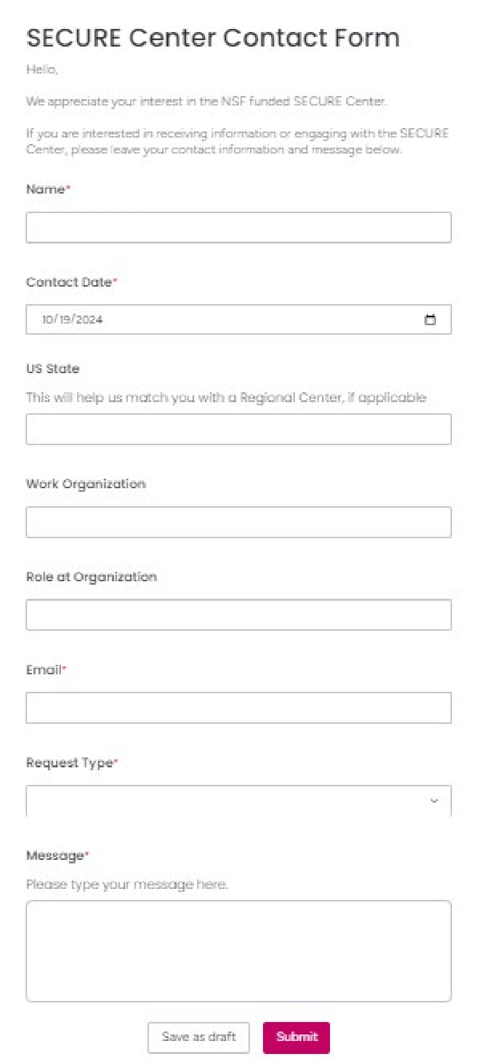
Safeguarding the Entire Community in the U.S. Research Ecosystem

Welcome to the SECURE Center,

We look forward to collaborating with the research community and stakeholders to provide support and services related to research security. We are in the initial stages of planning for the center and additional information will be available in the coming months.

Please continue to revisit this website periodically for additional information. We anticipate having specific details on ways that the research community can be involved with the SECURE Center in the coming months.

While we are in set up and planning mode for the center please share your interest level with us by completing and submitting the linked Interest/Contact Form.



SECURE Center Contact Form

Hello,

We appreciate your interest in the NSF funded SECURE Center.

If you are interested in receiving information or engaging with the SECURE Center, please leave your contact information and message below.

Name*

Contact Date*
10/19/2024

US State
This will help us match you with a Regional Center, if applicable

Work Organization

Role at Organization

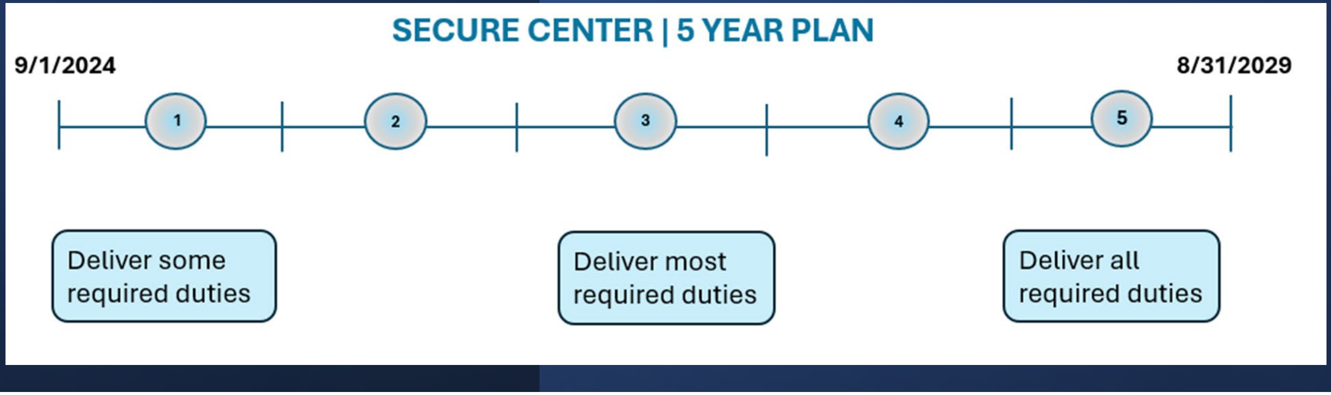
Email*

Request Type*

Message*
Please type your message here.

securecenter.uw.edu

Timelines & Deliverables



SECURE CENTER | 5 YEAR PLAN

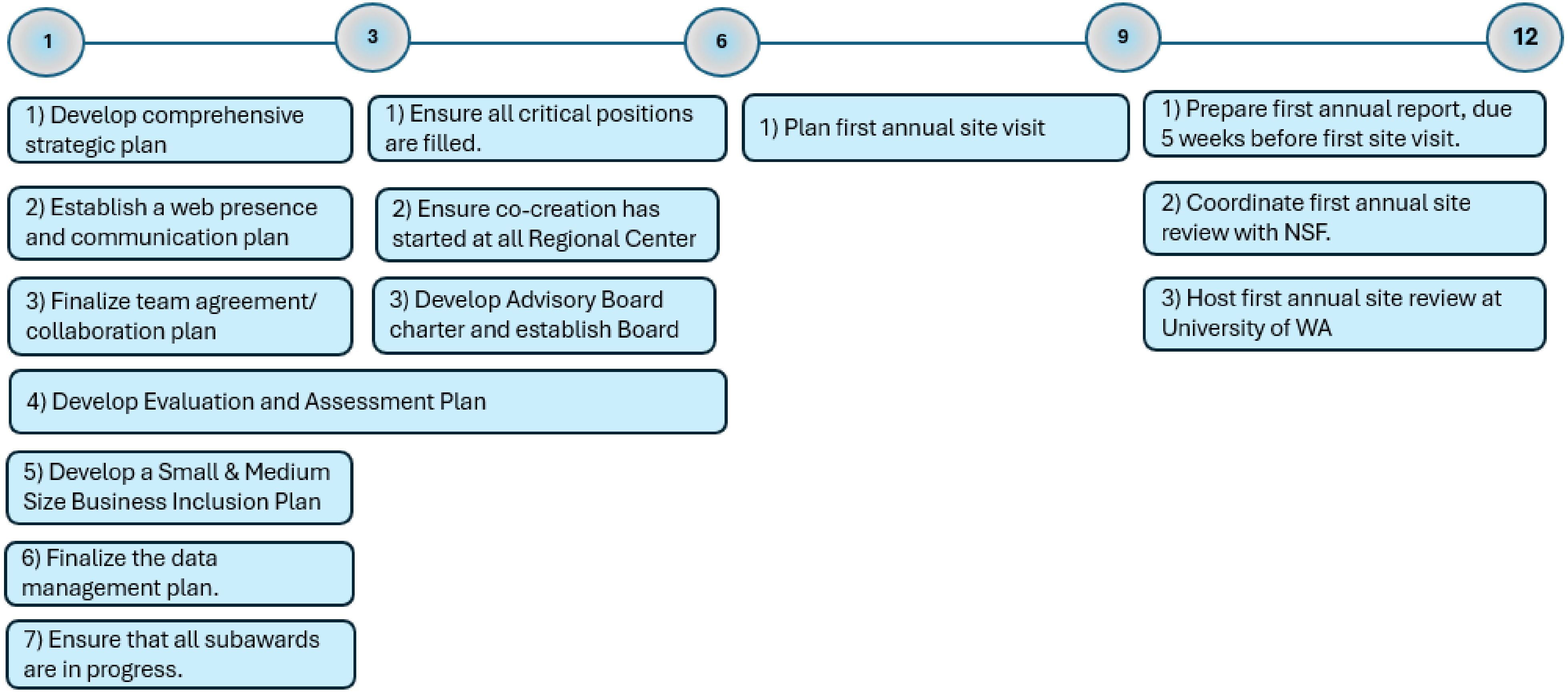
9/1/2024

8/31/2029

Deliver some required duties

Deliver most required duties

Deliver all required duties



1) Develop comprehensive strategic plan

2) Establish a web presence and communication plan

3) Finalize team agreement/ collaboration plan

4) Develop Evaluation and Assessment Plan

5) Develop a Small & Medium Size Business Inclusion Plan

6) Finalize the data management plan.

7) Ensure that all subawards are in progress.

1) Ensure all critical positions are filled.

2) Ensure co-creation has started at all Regional Center

3) Develop Advisory Board charter and establish Board

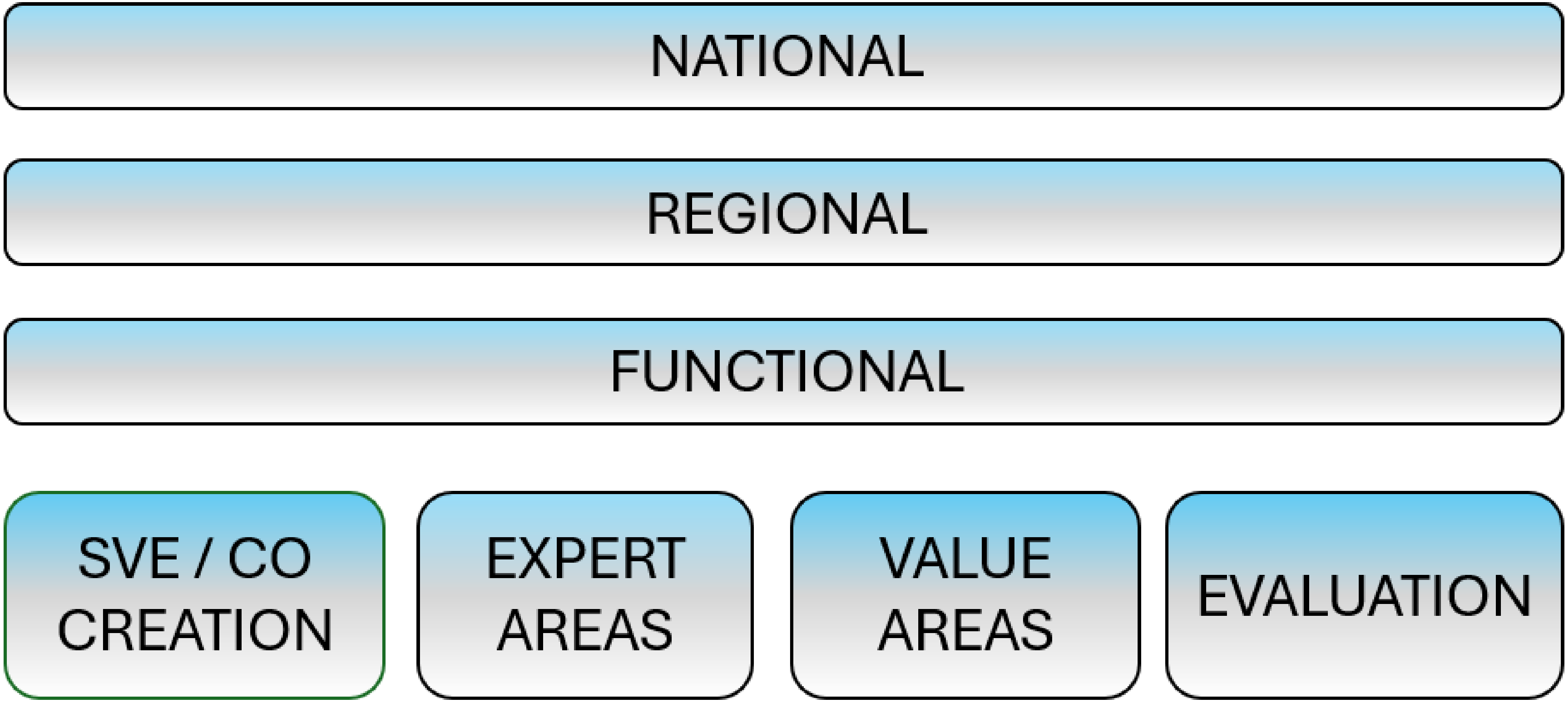
1) Plan first annual site visit

1) Prepare first annual report, due 5 weeks before first site visit.

2) Coordinate first annual site review with NSF.

3) Host first annual site review at University of WA

SECURE Center | Structure



NATIONAL

REGIONAL

FUNCTIONAL

SVE / CO CREATION

EXPERT AREAS

VALUE AREAS

EVALUATION

SECURE Center | Structure

NATIONAL

Director and Co-Director (Mark Haselkorn & Lynette Arias)

Advisory Board Chairs (Christina Ciocca Eller & Bob Sharp)

Office of the Director (Lisa Nichols, Jim Luther, Robert Nobles)

REGIONAL CENTERS

NORTHEAST – Northeastern University (Amanda Humphrey & Robin Cyr)

SOUTHEAST – Emory (Deepika Bhatia & David Sundvall)

MIDWEST – University of Missouri (Tony Caruso & Michele Kennett)

SOUTHWEST – University of Texas San Antonio & Texas A&M University
(Lori Ann Schultz & Kevin Gamache)

WEST – University of Washington (Lynette Arias & James Pierce)

SECURE Center | Structure

FUNCTIONAL AREAS

CO-CREATION/DESIGN

University of Washington (Sonia Savelli, James Pierce, Brie Yost, Bill Cornell),

Regional Center Design Leads

EXPERT AREAS

Mississippi State University (Narcisa Pricope and Chris Jenkins), Stanford Hoover Institute (Glenn Tiffert),

University of Michigan (Jason Owen-Smith and Lisa Nichols)

VALUE AREAS

University of Michigan (Lisa Nichols), College of Charleston (Susan Anderson), MindCette LLC (Kelly Shaver),

Stanford Hoover Institute (Frances Hisgen), and University of Washington (David Ribes)

EVALUATION

The Ohio State University (Caroline Wagner and Lisa Frazier), University of Washington (Sonia Savelli)

Questions & Discussion