BRIDGING THE GAP: HOW WEAK RESEARCH SECURITY POLICIES UNDERMINE INSTITUTIONAL COMPLIANCE

Brandon Strickland
Associate Vice President of Research Administration

Jennifer Keller
Director of Academic Research Security Compliance

Georgia Institute of Technology

CONTEXT AND URGENCY FOR UNIVERSITIES

WHY GOVERNANCE NOW DETERMINES RESEARCH SECURITY COMPLIANCE

- Federal Scrutiny and Compliance
  - Federal sponsors increasingly link research security governance – not just technical safeguards – to funding eligibility, and institutional credibility.
- Decentralization Requires Governance
  - Universities distributed authority and academic autonomy demand **clear governance structures** to consistently apply requirements like CMMC across campuses.
- Governance Shift
  - Research Security compliance has moved beyond IT and now depends on institution-wide policies, defined ownership, and repeatable execution.
- Risks of Weak Governance
  - Weak policies increase exposure to enforcement actions, reputational harm, and False Claims Act libility.

UNDERSTANDING RESEARCH SECURITY COMPLIANCE THROUGH A GOVERNANCE LENS

COMPLIANCE REQUIRES INSTITUTIONAL MATURITY, NOT JUST TECHNICAL CONTROLS

- Compliance is a Maturity Model
  - Compliance depends on embedding security requirements into institutional governance – not treating them as a checklist of technical controls
- Governance Hierarchy Matters
  - Effective compliance flows from clear policy, implemented through procedures, enforced by controls, and supported by evidence.
- Policy is a Common Failure Point
  - Ambiguous or inconsistent policies create downstream confusion and prevent repeatable, defensible compliance.
- Mature Governance Enables Readiness
  - Clear policies align expectations across research, IT, and administration, supporting consistent implementation.

POLICY GAPS AND THEIR OPERATIONAL CONSEQUENCES

POLICY GAPS RESULT IN COMPLIANCE FAILURES

- Unclear System Boundaries
  - Vague policies prevent clear definition of system boundaries, causing disputes over data scope and delays in security planning.
- Inconsistent Access Control
  - Missing role-based access policies lead to inconsistent controls and increase risk of access control failures during assessments.
- Incomplete Incident Response
  - Narrow incident response policies overlook research-specific breaches, causing risks in data incident handling and reporting.
- Insufficient Training Policies
  - Generic training without role-specific mandates and tracking fails to meet compliance and weakens security practices.

UNCLEAR SYSTEM BOUNDARIES

- CUI handling is not scoped during proposal review, leading researchers, IT, and administrators to assume different storage and access environments. After award, multiple systems are discovered in scope, triggering delays, rework and compliance risk.

- Discuss possible mitigation strategies.

INCONSISTENT ACCESS CONTROLS

- A research project handling CUI relies on departmental practices rather than a consistent, policy-driven access model. The PI grants a visiting scholar access to shared folders based on academic role rather that employment status. An assessment reveals varying privilege levels with no centralized record of enforcement – creating audit findings.

- Discuss possible mitigation strategies.

INCOMPLETE INCIDENT RESPONSE

- A research project handling CUI experiences a spill involving a graduate student account used to access project data. The department reports the issue to central IT, which resets credentials and closes the ticket. However, no notification is made to the research compliance team, and no determination documents as to whether CUI was access or exfiltrated. Months later, the institution cannot demonstrate timely incident reporting, escalation, or contractual notification required under the award – raising concerns about compliance and transparency.

- Discuss possible mitigation strategies.

INSUFFICIENT TRAINING POLICIES

- A university accepts a DARPA research award that includes a CUI Guide. While the institution has an annual cybersecurity awareness training, there is no role-based training requirement for researchers, graduate students, or departmental administrators involved in CUI-supported projects. New project staff begin work without received training specific to CUI-handling requirements. During a later assessment, the institution cannot demonstrate that personnel with CUI access were training on contract-specific requirements, raising concerns about compliance readiness and the reliability of institutional certifications.

- Discuss possible mitigation strategies.

ENFORCEMENT AND FUNDING SCRUTINY

LESSONS FROM RECENT UNIVERSITY ENFORCEMENT ACTIONS

- Cybersecurity Case
  - Federal enforcement actions highlighted gaps in institutional oversight of cybersecurity and research controls supporting federally sponsored research. Findings emphasized the absence of clearly documented system security expectations and governance mechanisms across research activities.
- Funding Scrutiny
  - Congressional review paused $17 million NSF funding due to concerns over international collaborations and governance.
- Governance and Reputation Risks
  - Across cases, weaknesses in governance – not just technical controls – created enforcement exposure, funding disruption, and reputational harm for institutions.

COMPLIANCE TRIGGERS

CUI IS NOT THE ONLY COMPLIANCE TRIGGER

Foreign Collaborations – Disclosure Obligations

Participation by foreign institutions, researchers, or funding sources trigger sponsor disclosure requirements.

International Travel or Appointments

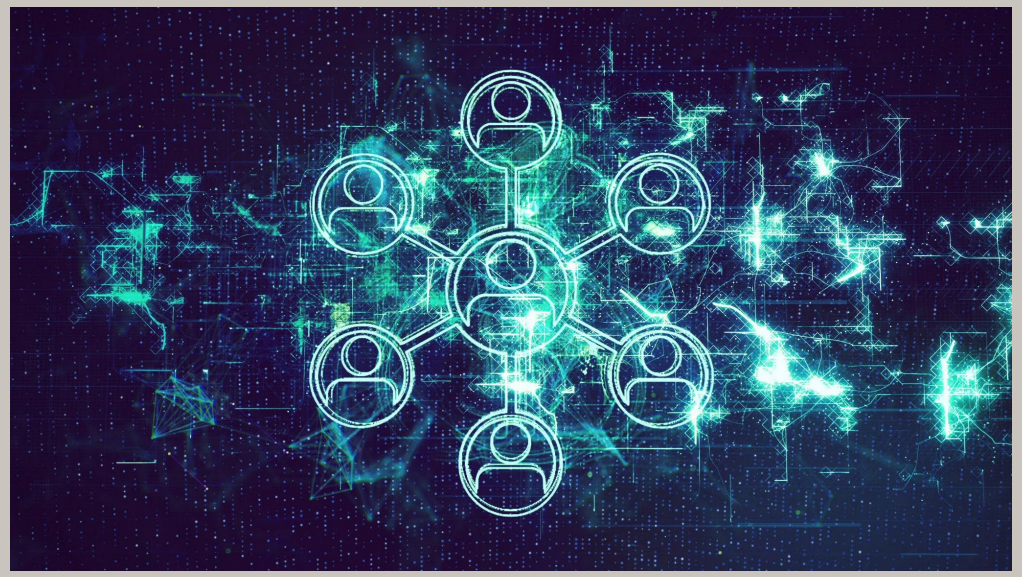
Foreign travel, visiting appointments, or honorary positions may trigger pre-approval, disclosure, or review requirements.

Export-Controlled Technologies

Research involving controlled technologies or data may trigger export control reviews, technology control plans, or licensing requirements.

LEADERSHIP AND RESEARCH ADMINISTRATION AS ENABLERS

BUILDING SUSTAINABLE RESEARCH SECURITY THROUGH GOVERNANCE AND POLICY



- Leadership Sets Direction and Accountability
  - Active leadership establishes clear ownership, authority, and expectations.
- Policy is Foundation for Sustainability
  - Clear, enforceable policies translate external requirements (CMMC, CUI, disclosures, export controls) into consistent institutional practice.
- Standardized Boundaries Enable Consistency
  - Defined system boundaries and approved research environments reduce ad-hoc decisions and post-award disruption
- Governance Enables Repeatable Execution
  - Formal governance structures support risk decisions, exception management, change control, and transparent oversight.

GOVERNANCE IS WHERE THE CONVERSATION BEGINS

COMPLIANCE DEPENDS ON CLEAR POLICY, DEFINED OWNERSHIP, AND CONSISTENT EXECUTION ACROSS THE LIFECYCLE

WE WELCOME YOUR QUESTIONS AND DISCUSSION ON

- Where governance gaps create the most risk
- How institutions are operationalizing emerging requirements
- What contracting officers and sponsors expect to see – and why
- How is your institution governing its research security obligations today

THANK YOU

Please reach out to continue the conversation…

- Reach Brandon Strickland at brandon.Strickland@osp.gatech.edu
- Reach Jennifer Keller at jkeller63@gatech.edu