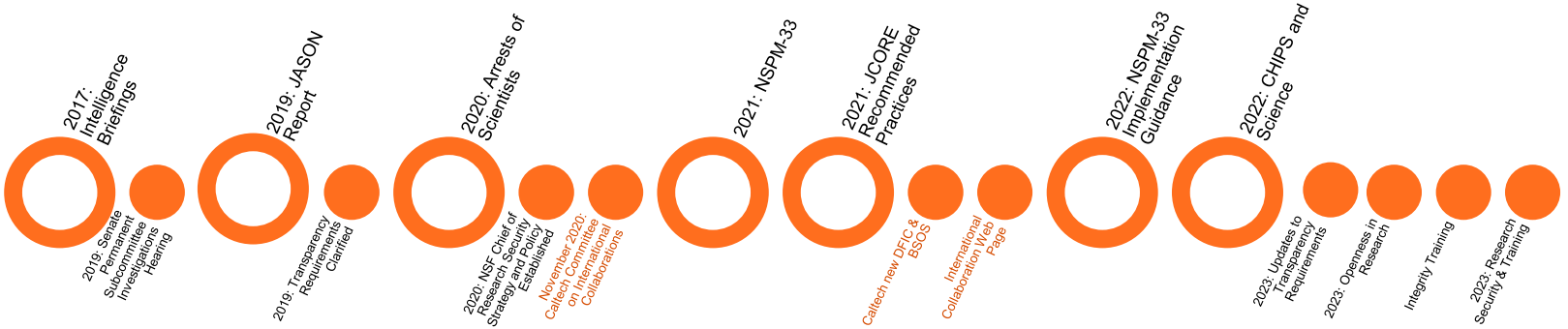
Foreign Engagement and Research Security

Grace Fisher-Adams, Chief Research Policy Officer
Jin Chang, Chief Information Officer

March 6, 2023

Caltech

Research Security Timeline



Caltech

National Security Presidential Memo
NSPM-33
(January 2020)

1. Enhance Awareness of Research Security Risks and Protections
2. Strengthen Disclosure Requirements and Processes
3. Limit Access and Participation (Research Security)
4. Vet Foreign Students and Researchers
5. Information Sharing (Between Agencies About Violations)
6. Training (Integrity/Cybersecurity/Research Security/Export)
7. Risk Identification and Analysis
8. Promote and Protect International R&D Cooperation

Caltech

Report of the faculty committee on international collaboration

(November 3, 2020)

Kaushik Bhattacharya, Bethany Ehlmann, Cathy Jurca, Jennifer Lum, Steve Mayo,
Dan Meiron (chair), Tom Prince, Dick Seligman, Zhen-Gang Wang, Jonas Zmuidzinas

Ten Recommendations to ensure continued foreign collaboration guided by policies and practices of transparency, reciprocity and research integrity

- Focus on Financial Interest and Commitment Disclosure, Training, and Better Understanding of Disclosure Requirements
- Develop criteria and practices for foreign scholars to know whether they are in a foreign government talent program
- Encourage openness: Caltech should not engage in agreements that exclude foreign nationals in sponsored research

Caltech

Dislcosure Proposals and Awards

Dislcosure Financial Interests and Commitments

Research Integrity

Research Security

Requirement	T	I	TR	RS	FE	NSPM33	NSPM Recommen	NSPM Implement	CHIPS	NSF PAPPG	Wolf Amd	In Effect?	Caltech	Links to References			
												P. Common Form (Other Agencies)					
Biosketch: Affiliations, Positions/Appointments	x			x	x	2		1,1a		1, 1a		Y. Use Tables as Guidance (NSF/NIH) P. Common Form (Other Agencies)		NSF Table	NIH Table		Proposed Common
Other Support: C&P, In-kind, Visiting Scholar Funding, SPD External Funding, Travel for Research; Facilties and Other Resources	x			x	x	2		1,1a		1, 1b		Y. Use Tables as Guidance (NSF/NIH) P. Common Form (Other		NSF Table	NIH Table		Proposed Common
Continuing Other Support Disclosure Reporting: JIT, Annual & Final Reports	x			x	x	2		1,1a		1, 1a, 1b, 1c		Y. NIH/NSF See PAPPG and NIH GM P. (Other Agencies)		PAPPG 23	GPS (2.5.1 and 8.4.1.9)		
Biosketch/Other Support Disclosers: PI, Senior/Key Personnel	x			x	x	2		1,1a		1, 1a, 1b, 1c		Y. NIH/NSF See PAPPG and NIH GM P. (Other Agencies)		PAPPG 23	GPS (8.4.1.8)		
Certifications: Biosketch/Other Support	x			x	x	2		1,1a		2		Y. NIH/NSF See PAPPG and NIH GM P. (Other Agencies)		PAPPG 23	GPS (8.4.1.8)		
Foreign Component					x							Y. NIH			NIH NOT		
Report FGTP/Malign FGTP	x			x	x	2,3	6, 10	1,1a				Y. FGTP: NSF See PAPPG (Senior Personnel); NIH See NOT and GPS; DOE, DARPA See Proposal P. (FGTP: Other Agencies;		PAPPG 23	GPS		
Prohibit FGTP				x	x	2,3	10		8			Y. DARPA & DOE (See Proposal)					
Prohibit Malign FGTP				x	x	2,3	10		8,9			Y. DARPA & DOE (See Proposal) P. Other Agencies by (Rule by					
Copies of Foreign Agreements	x			x	x				10			Y. NIH and NSF		PAPPG	NIH NOT		
Consequences of Violations of Disclosure Requirements	x			x	x	2	16	3	10			Y. NSF See PAPPG P. (Other Agencies)		PAPPG 23			
DISCLOSURE FINANCIAL INTERESTS AND COMMITMENTS																	
Institutional FCOI and COC Policy	x				x	2	5	1,1a				Y. NIH, NSF, DOE P. NASA, Other Agencies	COI Policy, Fed COI Policy, Faculty Handbook, PM Outside		42 CFR 50		
SFI and Commitment Disclosure Required	x	x			x	2	6	1,1a		2a		Y. Required for "Investigators" P. (Broaden to Covered Individuals) Include Grad Students?	COI Policy/Fed COI Policy DFIC Disclosure	PAPPG 23	42 CFR 50	DOE FAL	
Reporting FGTP/Malign FGTP	x	x			x	2,3	6, 10	1,1a				Y. FGTP: NSF See PAPPG (Senior Personnel); NIH See NOT and GPS; DOE, DARPA See Proposal P. (FGTP: Other Agencies; MFGTP: All Agencies)	DFIC Disclosure				
FCOI and CoC Management	x	x			x			1,1a				Y. NIH/DOE and NSF: JIT P. NASA and Other Agencies	DFIC; JIT Review	PAPPG 23	42 CFR 50	DOE FAL	
Determining Award FCOI and Reporting	x	x			x	2		1,1a				Y. NIH/DOE and NSF: JIT P. NASA and Other Agencies	DFIC; JIT Review	PAPPG 23	42 CFR 50	DOE FAL	
Copies of Foreign Agreements	x				x				10			Y. NIH and NSF		PAPPG	NIH FCOI		
Certifications: Conflicts of Interest	x	x			x	2		1,1a		2		Y. NSF See PAPPG; NIH See NOT		PAPPG 23	NIH NOT		
Consequences of Violations of Disclosure Requirements	x			x	x	2	16	3	10			Y. NSF See PAPPG P. (Other Agencies)		PAPPG 23			
FCOI Training Requirement	x		x			6						Y. NIH			42 CFR 50		
RESEARCH INTEGRITY																	
Research Integrity Training		x	x			6	10		3	2b							
RESEARCH SECURITY																	
Institutional	x			x	x		1,2					P					
Institutional Requirements to support Research Security and Integrity		x		x			17					Some in place with enactment of CHIPS					
Designate Research Security Officer				x			4	5	1			P					
Centralized review and approval of formal research partnerships				x	x	7	18					P					
Prohibition of NSF for Institutions that host or support Confucius Institutes				x	x				6			Y. August 9, 2022					
Institute Certification that no researcher is part of Malign FGTP & all researchers made aware				x	x				14			P. (Rule by 8/2024)					
Cybersecurity				x	x		4	5, 5b				P					
Establish Data Security Measures				x	x		21					P					
Foreign Travel Security				x	x		4	5				P					
Risk-based review and guidance for foreign				x	x		19					P					
International Collaboration is Acceptable, except with institions on one of the restricted					x	8			14			Y. August 9, 2022					
Foreign Student and Researcher Review/Vetting/Management				x	x		4, 20	7	12, 15			P					
Consequences of Violations of Disclosure and Engagement Requirements	x			x	x	2	16	3				Y. NSF See PAPPG P. (Other Agencies)		PAPPG 23			
Export Control Training				x	x	1,6	4	5				P					
Research Security Training			x	x		1,6	4	5	11			Im. By August 2023 Modules Released					
Institute Certification the RS Training is in			x	x					11			Im.					
Cybersecurity Training			x	x		1,6	4	5				P					
Dept of Education Reporting of Foreign Gifts, Contracts, etc. (Sec 117)				x	x		9					Y.					
NSF Office of Research Security and Policy: Reporting of Foreign Gifts, Contracts, etc.				x	x		9		7			Im. Waiting for NSF to tell us where/how to report.					
Agency Information Sharing (about PI and violations)	x			x	x	5	4	4, 5	1,2,4			Y. NSF Established Research Security and Integrity Information Sharing					
Use Digital Persistent Identifiers	x			x	x		4,8	2				Y. SciENcv Im. Common Forms	OrcID, SciENcv				

KEY: T=Transparency; I=Integrity; TR=Training; RS= Research Security; FE=Foreign Engagement
In Effect: Im= Imminent; Y=Yes in Effect; P=Pending Regulation or Legislation

Caltech

Disclosure Requirements

Researcher

- Biosketch
- Other Support
- Facilities and Other Resources
- Foreign Components
- Foreign Government Talent Program[1]
- Financial Interests and Commitments (DFIC) Disclose and Receive Training
- Foreign Agreements
- Certify all disclosures are True and Correct
- Update Other Support Disclosure JIT, Annual and Final Reports
- Establish a DPI (OrcID or SciENcv profile)

Caltech

- Review DFIC for FCOI; Manage FCOI, Report
- Review Foreign Agreements
- Certify that Researcher Knows Disclosure Obligations
- Provide Tools:
  - DFIC: Disclose Significant Financial Interests, Commitments (Appointments & Professional)
  - BSOS: Active Awards, PD External Funding, Other Entries by PI and GM
  - eDAF: Will provide pending support
  - Grants Management Software

Agencies

- Provide Common Disclosure Form: Biosketch and Other Support: SciENcv
- Establish Consequences for Violations of Disclosure Requirements
- Provide distinct requirements regarding restrictions or prohibitions[1]
- Establish a federal organization and a database to share among agencies

[1] Foreign Government Talent Program (defined later)

Caltech

Caltech International Collaboration Webpage

- Webpage
  - https://researchcompliance.caltech.edu/international_collaboration
- Biosketch and Other Support Disclosure Tables
  - NSF: https://www.nsf.gov/bfa/dias/policy/disclosures_table/jan2023.pdf
  - NIH: https://grants.nih.gov/grants/forms/NIH-Disclosures-Table.pdf
- DFIC User Manual
  - https://researchcompliance.caltech.edu/compliance/conflicts-interest/coi-guide
- BSOS User Manual
  - https://researchcompliance.caltech.edu/documents/20676/BSOS-Guide.pdf
- Coming Soon: Foreign Government Talent Program Information

Caltech

Research Integrity and Data Sharing

Researcher

- Training for *all* Researchers in Responsible and Ethical Conduct of Research.
- Data Sharing Requirements (Open Science)
  - NSF in place for some time
  - NIH refreshed January 2023
  - DOE, USGS, NASA and many others issuing policies quickly

Caltech

- Provide Training:
  - CITI for Grad Students and Post Docs
  - **[NEW] for Faculty and Senior Staff (coming June/July 2023)**
- Library Support for Data Sharing

Agencies

- Require a Policy for Research Integrity Training
- Issuing Data Sharing Policies

Caltech

Research Security

Researcher

- Training in Research Security, Cybersecurity, and Export Control (as appropriate)
- Abide by Research Security Program Requirements
- Travel Reporting
- Limit or eliminate FGTP participation

Caltech

- Establish a Research Security Program
- Provide Training (Res Security, Cybersecurity, Export)
- Designate a Research Security Officer
- Centralized Review/Approval of Research Partnerships
- Monitor FGTP Activities. Prohibition of Malign FGTP.
- Disclose foreign contracts and gifts (Sec 117, CHIPS)
- Provide Certifications

Agencies

- Require a Policy for Research Integrity Training
- Clear requirements for restrictions/ prohibitions of activities (e.g. Confucius Institutes, NDAA lists, Malign Foreign Talent Programs)
- Establish a federal organization and a database to share among agencies (Information Sharing)

Caltech

Foreign Government Sponsored Talent Recruitment Program

An effort organized, managed or funded by a foreign government or its instrumentality to:

- Recruit science and technology professionals or students
- May attempt to acquire proprietary technology, software, unpublished data and or methods, and IP to further the military or economic goals of the foreign government.
- May incentivize the individual to relocate although some encourage continued employment in the US research facilities or use of US federal funding.
- Compensation can include cash, research funding, complimentary foreign travel, honorific titles, career advancement opportunities, promised future compensation, or other compensation, including in-kind compensation.

Not Necessarily Prohibited…

Caltech

Malign Foreign Government Talent Program

Program, position or activity that requires an individual to take on the following:

- Unauthorized transfer of intellectual property or other nonpublic information; or
- Recruit trainees or researchers to enroll in such program; or
- Establishing a laboratory/employment/appointment in a foreign country in violation of terms and conditions of a Federal research award; or
- Inability to terminate; or
- Overcapacity/overlap/duplication; or
- Mandatory to obtain research funding from the foreign government's entities; or
- Omitting acknowledgement of U.S. home institution/funding agency; or
- Not disclosing program participation; or
- Conflict of interest/commitment;

Will Be Prohibited (CHIPS)…

AND

- Sponsored by a country of concern (PRC, Iran, Russia, N. Korea)

Caltech

Research Security Program

- Designate a Research Security Officer
- Components:
  - Foreign Travel Security
    - Significant Financial Interest (Reimbursed travel is considered an financial interest reportable to Caltech if you have NIH or DOE funding) Travel
    - Other Support (Reimbursed travel supporting travel to perform research anywhere is considered other support and must be reported NSF, NIH)
    - *Institutional International Travel Policy*
    - *Registration/Recordkeeping (of "faculty and staff") who will travel internationally for organizational business, teaching , conferences, research purposes, or any travel that would put a person at risk. As appropriate, may require disclosure before travel, approval, briefings, and assistance with e-device security.*
  - Research Security Training
  - Export Control Training
  - Cybersecurity
    - Assessment of Risk with regard to Research Data

Caltech

Research Security Risk Assessment

- Data Types (Library Survey)
- Risks
  - Sponsor Requirements
  - Contractual Requirements
  - Human Data
  - Intellectual Property
  - Institute Privacy/Reputational Risk
  - Financial Risk
  - Loss of Time & Effort/Data Loss/Reproduction
  - Operational Risk (e.g. Ransomware)
  - Other Risks?
- Cyber Security Controls
- Cybersecurity Committee Review and Recommendations

Data Type	Data Source	Sponsor Security Requirements: (Export Control, CUI/CMMC, etc)	Contractual Risk (NDA, MTA, etc.)	Human Subjects (HIPAA)	Human Subjects (PII-privacy)	Intellectual Property	Institute Privacy / Reputational Risk	Financial Risk	Research Operations / Operational Risk (Ransomware)	Other Risks?
e.g., Gene Expression Data	Human		x	x	x	?	x	x	x	x
IT Security Controls (TBC)		Follow Sponsor Requirement	Follow Contract Requirement	HIPPA Regulations	**What Cybersecurity Controls Apply?**					

Caltech

Cyber Security Controls

(based on NSPM-33 implementation guidelines)

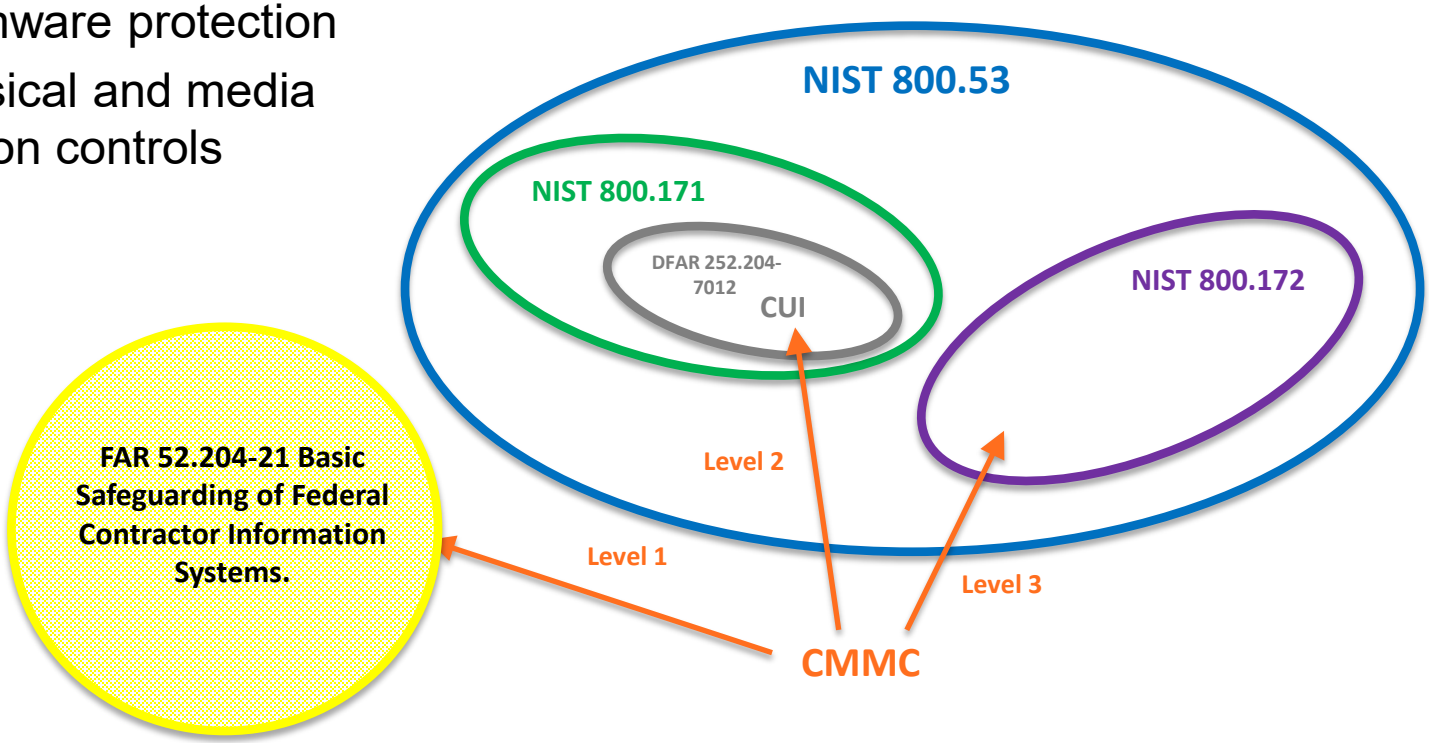
NSPM-33 implementation guidelines for Research Security outlines 14 cyber security elements from "access control", "identification & authentication", "system communication protections" and "system information integrity" domains

1. **Provide regular cybersecurity awareness training for authorized users of information systems, including in recognizing and responding to social engineering threats and cyber breaches.**
2. Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
3. Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
4. Verify and control/limit connections to and use of external information systems.
5. Control any non-public information posted or processed on publicly accessible information systems.
6. Identify information system users, processes acting on behalf of users, or devices.
7. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
8. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
9. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
10. **Provide protection of scientific data from ransomware and other data integrity attack mechanisms**.
11. Identify, report, and correct information and information system flaws in a timely manner.
12. Provide protection from malicious code at appropriate locations within organizational information systems.
13. Update malicious code protection mechanisms when new releases are available.
14. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Caltech

NSPM-33 cyber security elements are:

- **Verbatim copy of CMMC Level 1, FAR52.204-21 except**
  - Cyber security training
  - Ransomware protection
  - No physical and media protection controls



Caltech

Access Control
Establish who has access to your system and how to control privileges

Identification & Authorization
Ensure the proper authentication and roles

System Communication Protection
Control the communication at system boundaries

System Information Integrity
Manage flaws and monitor network and systems

Resnick HPC Cyber Security Controls (summary)

- **Cyber security training** (optional)
- **Process**: HR on-boarding process
- **Authentication**: Caltech credential + 2FA (Duo)
- **Access**: Campus network or VPN access only
- **Authorization**: **No administration** access, layered permission (PI, individual users, group shared drive)
- **System Boundary**: Campus border router, host-based firewall, separate private network and dedicated file transfer node
- **Monitoring**: Periodic scanning, event logging and resource-used statistics
- **Support**: central HPC support & information security teams
- **Endpoint protection** : CrowdStrike EDR (endpoint detection and response) scheduled

Additional Opportunities

- Renick Central HPC
  - Research data backup and storage is up to individual PI
  - The Individual researcher also owns cyber security element #5, "*Control any non-public information posted or processed on publicly accessible information systems*"

- Cyber security controls and guidelines for ensuring research data security for non-centrally managed systems?

Caltech

Thank you!

Caltech