Security Tomorrow, Today: Cybersecurity Updates from DARPA

June 5, 2025

COGR℠

Advancing Effective Research Policy

www.cogr.edu

www.linkedin.com/company/cogr

#COGRJune25

Securing Tomorrow, Today: Cybersecurity Updates from DARPA

June 5, 2025

Speaker:

Jesse Watkins, Deputy Director, Security and Intelligence Directorate, Defense Advanced Research Projects Agency (DARPA)

Moderator:

Kris West, Director, Research Ethics & Compliance, COGR

COGR

Cybersecurity Challenges for Academic Institutions Working with Controlled Unclassified Information (CUI)

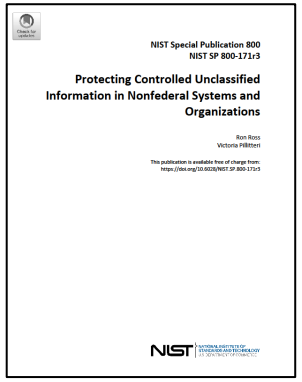
Jesse Watkins
Deputy Director, Security and Intelligence Directorate

Briefing prepared for: Council of Government Relations (COGR)
Research Ethics & Compliance (REC) and Research Security and Intellectual Property (RSIP) Committees

4-5 June 2025

Information Technology (IT) Cybersecurity Requirements

- **NIST SP 800-171 Rev 3** (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)
  - Compliance required for protection of USG CUI data and information
  - 800-171 security requirements represent a subset of the controls that are necessary to protect the confidentiality of CUI


NIST Special Publication 800
NIST SP 800-171r3

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Ron Ross
Victoria Pillitteri

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3

NIST

Table 1. Security Requirement Families

Access Control	Maintenance	Security Assessment and Monitoring
Awareness and Training	Media Protection	System and Communications Protection
Audit and Accountability	Personnel Security	System and Information Integrity
Configuration Management	Physical Protection	Planning
Identification and Authentication	Risk Assessment	System and Services Acquisition
Incident Response		Supply Chain Risk Management

Microsoft Excel Worksheet

NIST SP 800-171A R3

  - Government Organizational-Defined Parameters
    - Provide both the flexibility and specificity needed by organizations to clearly define their CUI security requirements, given the diverse nature of their missions, business functions, operational environments, and risk tolerance
    - Support consistent security assessments in determining whether specified security requirements have been satisfied

- **NIST SP 800-171A Rev 3** (Assessing Security Requirements for Controlled Unclassified Information)
  - Assessment of institution IT network/system needs accomplished to identify areas of non-compliance

Cybersecurity Maturity Model Certification (CMMC)

- CMMC provides the DoD with increased assurance that contractors and subcontractors are meeting the cybersecurity requirements for nonfederal systems processing controlled unclassified information.

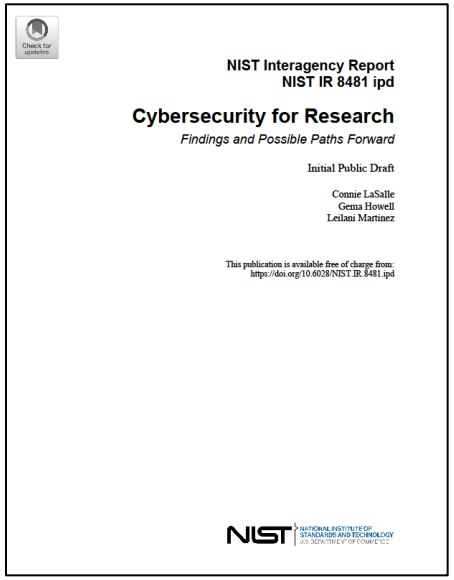
- Tiered System
  - Level 3 (Higher-Level Protection of CUI Against Persistent Threats)
    - 134 requirements [110 from NIST SP 800-171, 24 from NIST SP 800-172] (DFAR clause 252.204-7012)
    - Level 2 Certification pre-requisite
    - DIBCAC Certification Assessment every 3 years
    - Annual Affirmation

  - Level 2 (Broad Protection of CUI) – **Current DARPA Standard for Industry Performers**
    - 110 requirements (DFAR clause 252.204-7012)
    - C3PAO Certification Assessment every 3 years, or
    - Self Assessment every 3 years, certain programs
    - Annual Affirmation

  - Level 1 (Basic Safeguarding of CUI)
    - 15 requirements (FAR clause 52.204-21)
    - Annual Self Assessment
    - Annual Self Affirmation

Cybersecurity Challenges and Risks

- **NIST IR 8481** (Cybersecurity for Research: Findings and Possible Paths Forward)
  - Awareness - General cybersecurity awareness is lacking
  - Workforce - IT security workforce challenges
  - Culture clash – Compliance culture vs Risk Management culture
  - Limited budgets for cybersecurity - struggle to provide the resources needed
  - Complicated requirements landscape – difficult to decipher, may vary depending on organization, may not address relevant risk
  - Rapid pace of innovation - niche tool stacks that need to be protected, security professional capabilities, and the technologies available to adversaries
    - Biotechnology
    - Quantum Computing
    - Neural Psychology
    - Optical Science
    - Space research
    - Engineering
    - Clinical research


NIST Interagency Report
NIST IR 8481 ipd

Cybersecurity for Research

Findings and Possible Paths Forward

Initial Public Draft

Connie LaSalle
Gema Howell
Leilani Martinez

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8481.ipd

NIST

Emergent Technology Challenges

- The handling of specialized, sensitive, and/or regulated data, such as protected health information (PHI), controlled unclassified information (CUI), and data related to International Traffic in Arms Regulations (ITAR), which may require additional controls, reporting, or education regarding usage
- The need for inter-institutional and international collaboration, which may require additional investments in identity and access management to appropriately support research while protecting confidentiality
- The distributed accountability for cybersecurity, which is reinforced through research agreement language and institutional processes, politics, and cultures
- The unique characteristics and configurations of the research equipment involved and the lack of secure storage and other tools that meet regulatory and contractual requirements
- The lack of institutional capacity to support required research tools (e.g., Research Electronic Data Capture, or REDCap)

NIST Recommended Solutions to Challenges

- **Targeted cybersecurity resources**
  - Developed resources that are specific to particular fields of research and could emphasize the risks, impacts, and importance of applying cybersecurity within the research context.
- **Collaborative engagements**
  - Collaborating with existing research communities and the need for more collaboration with Federal Government entities. (e.g. EDUCASE HEISC, NSF RRCoP, Trusted CI, RENH-ISAC, National Laboratories)
- **Training**
  - Training 431 resources designed for researchers and their teams could raise awareness about the importance of cybersecurity, particularly cybersecurity's value in preserving data integrity.
- **Guidance for frameworks**
  - Tailoring certain frameworks to support research environments could help ease the integration of cybersecurity while simplifying the process and minimizing operational overhead.
- **Grant guidance for security compliance**
  - Effective grant writing guidance that considers security, compliance, and research environments hosted at higher education institutions.
- **Shared services support**
  - Increasing awareness of available shared service opportunities and developing trusted cybersecurity services can help mitigate limited cybersecurity budgets for many institutions

Q&A Submitted by COGR REC & RSIP

- Q1: Overview of any plans that DARPA has for requiring institutions to implements NIST 800-171?
  - A1: DARPA is not planning on a mandatory implementation of NIST 800-171 for academic institutions. However, more programs being solicited are requiring data protection. Some programs may be "fundamental research," but could evolve into CUI levels depending on success of research.
- Q2: How do DARPA's plans regarding NIST 800-171 fit in with the larger joint agency/OSTP efforts to develop cybersecurity standards based on NIST IR 8481 for mandated research security programs?
  - A2: OSTP guidelines for implementation of cybersecurity requirements state that *"Institutions of Higher Education (IHE) will have one year after the publication of the NIST document to implement a cybersecurity program that meets the document's requirements."*
  - NIST 8481 "*does not identify a specific cybersecurity framework or set of practices that institutions are required to follow. Rather, it constitutes a summary of the study used to create NIST IR 8481, a description of broad categories risks and challenges that research institutions face in the cybersecurity landscape, recommendations for future work, and next steps, along with an appendix of NIST resources for managing cybersecurity risks.*"
  - DARPA uses NIST 800-171/172 as the cybersecurity framework to protect CUI.
- Q3: NIH required institutions to implement NIST 800-171 standards for certain genomic data, but it did not consider this information to be CUI. Will DARPA take a similar approach, or, alternatively, will it consider any information that it subjects to the NIST 800-171 standard to be CUI and therefore subject to other CUI requirements?
  - A3: NIST 800-171 is a framework tailored to protect USG defined CUI. However, it is also used as a recommended framework to help industry/academia protect their unclassified networks with basic cybersecurity. Genomic data that is categorized as CUI by DARPA will be identified in a program specific CUI Guide issued by the tech office.

Q&A Submitted by COGR REC & RSIP (cont)

- Q4: Will DARPA mandate that NIST 800-171 be applied to all facets of a grantee's IT systems, or will it limit implementation only to those components/sectors of the systems that handle information that DARPA subject to the NIST 800-171 standard?
  - A4: DARPA only intends to apply the NIST 800-171 standards to those systems that directly handle data that requires specific protections. This can be done through a partitioned section of the institution's networks or other controls agreed upon by the PSO and institution's ISSO/ISSM. (However, application to the entire institution's IT system is considered a best practice.)
- Q5: When NIH began requiring NIST 800-171 for certain genomic data, it accepted either Rev. 2 or Rev. 3 of this standard, until it notified grantees otherwise. Will DARPA take a similar approach, or will it require compliance with Rev. 3 at initial implementation?
  - A5: If an institution has already began implementation using R2 it may continue to use that standard. If they have not, R3 would be required as the newest version. However, it is recommended to implement R3 as soon as practical.
- Q6: Will DARPA require an independent assessment of a grantee institution's compliance with NIST 800-171? If so, will it require the assessment to be conducted by an external reviewer, or will an independent internal reviewer (e.g., internal audit) be acceptable?
  - A6: DARPA is in the process of implementing CMMC (as described earlier). As the standard requirement is Level 2, self-assessments may be authorized. If an external assessment is required, it would be following the CMMC requirement for a C3PAO Certified Inspector.
- Q7: NIH permitted institutions that needed to bring the components of their systems handling data that NIH subjected to NIST 800-171 to provide plans of action and milestones (POAMs) as demonstrations of compliance with the new standard. Would DARPA consider a similar approach.
  - A7: Yes, if you are working on a Level 2 CMMC requirement. Level 1 does not allow for a POAM due to the minimal requirements of controls.

DARPA Fundamental Research Risk-Based Security Reviews (FRRBS)

New OUSD(R&E) Decision Matrix Summary of Changes

Category	Location	Change Summary	Rationale
New Law	Page 1 and Factor 4	Prohibits FY25 funds for proposals involving entities on the 1286 list	Section 238 of the FY25 NDAA
Implementation	Page 1 and Factor 1	Removed prohibition lined to institutional MFTRP policies; clarified co-authorship considerations	No statutory requirement for institutional policies; co-authorship alone isn't grounds for rejection
Date Updates	Various	Updated date references throughout to reflect current law and policy	Various reasons, including passage of deadlines, clarification of effective dates, and broader application of policies
Definitions	Definitions and Factor 4	Removed “Association”, revised “Affiliation” definition for clarity	Components expressed uncertainty on differences; streamlined for clarity.
Administrative	Throughout	Title updated to "2025"; clarified "Mitigation Measures Expected"; general language revisions	Clarity and accuracy

New OUSD(R&E) Decision Matrix

	Factor 1: Foreign Talent Recruitment Programs	Factor 2: Funding Sources	Factor 3: Patents	Factor 4: Entity Lists
Prohibited factors	Indicator(s)[1] of active participation[2] in a malign foreign talent recruitment program (MFTRP).	**None**	**None**	**For FY 2025:**[3] Collaborations for the specific purpose of fundamental research[4] between institutions of higher education and academic institutions that are included in the most recently updated list developed pursuant to section 1286 of the NDAA for FY 2019, as amended, or employees of such institutions.[5]
Factors discouraged by DoD policy, mitigation measures required, rejection of proposal required if no mitigation possible	**None**	Indicator(s) that the covered individual is currently receiving funding from a Foreign Country of Concern (FCOC) or an FCOC-connected entity.	Patent application(s) or patent(s) not disclosed in proposal, that resulted from research funded by the U.S. Government (USG), that were filed in an FCOC prior to filing in the United States or filed on behalf of an FCOC-connected entity.	**For the period after Aug 9, 2022:**[6] Indicator(s) of affiliation with an entity on the version at the time of review of the U.S. Bureau of Industry and Security (BIS) Entity List,[7] the Annex of Executive Order (EO) 14032[8] or superseding EOs, section 1260H of the NDAA for FY 2021,[9] or section 1286 of the NDAA for FY 2019, as amended.
Mitigation measures expected	**For the period between Oct 10, 2019[10] and Aug 9, 2024:** Indicator(s) of participation in an MFTRP meeting any of the criteria in section 10638(4)(A) of the CHIPS and Science Act of 2022.	**For the period after Oct 10, 2019:** Indicator(s) that the covered individual received funding from an FCOC or an FCOC-connected entity.	Patent application(s) or patent(s) disclosed in proposal resulting from research funded by the USG that were filed in an FCOC, or on behalf of an FCOC-connected entity, prior to filing in the United States.	**For the period between Oct 10, 2019 and Aug 9, 2022:** Indicator(s) of affiliation with an entity on the current version of the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, section 1260H of the NDAA for FY 2021, or section 1286 of the NDAA for FY 2019, as amended.
Mitigation measures suggested	**For the period after Oct 10, 2019:** Covered individual's co-author(s)[11] on publications in scientific and engineering (S&E) journals are participants in an MFTRP meeting any of the criteria in section 10638(4)(A) of the CHIPS and Science Act of 2022. **For the period of 10 years prior to Oct 10, 2019:** Indicator(s) of participation in an MFTRP meeting any of the criteria in section 10638(4)(A) of the CHIPS and Science Act of 2022.	**For the period of 10 years prior to Oct 10, 2019:** Indicator(s) that the covered individual received limited or partial funding from an FCOC or an FCOC-connected entity.	Patent application(s) or patent(s) not disclosed in fundamental research project proposal that resulted from research funded by the USG that were filed in a non-FCOC, or on behalf of an entity in a non-FCOC, prior to filing in the United States. **or** Co-patent(s) application(s) with a person on the U.S. BIS Denied Persons List.[12] **or** Co-patent(s) applications(s) with an individual affiliated with any entity on the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, section 1260H of the NDAA for	**For the period of 10 years prior to Oct 10, 2019:** Indicator(s) of affiliation with an entity on the current version of the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, section 1260H of the NDAA for FY 2021, or section 1286 of the NDAA for FY 2019, as amended. **For the period after Oct 10, 2019:** Covered individual's co-author(s) on publications in S&E journals are affiliated with an entity on the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, section 1260H of the NDAA for FY 2021, or section 1286 of the NDAA for FY 2019, as amended. Covered individual is a co-author on a publication in an S&E journal with a person(s) on the U.S. BIS Denied Persons List.

New OUSD(R&E) Decision Matrix (cont)

			FY 2021, or section 1286 of the NDAA for FY 2019, as amended.	
No mitigation needed	No indicator(s) of participation in an MFTRP meeting any of the criteria in section 10638(4)(A) of the CHIPS and Science Act of 2022.	No indicator(s) that the covered individual is receiving, or has received, funding from an FCOC or an FCOC-connected entity.	All patent applications or patents resulting from research funded by the USG have been filed in the United States prior to filing in any other country.	No indicator(s) of any affiliation with an entity on the U.S. BIS Entity List, the Annex of EO 14032, or superseding EOs; section 1260H of the NDAA for FY 2021; or section 1286 of the NDAA for FY 2019, as amended. No indicator(s) that a covered individual's co-author(s) on publications in S&E journals are affiliated with an entity on the U.S. BIS Entity List; the Annex of EO 14032 or superseding EOs; section 1260H of the NDAA for FY 2021; or section 1286 of the NDAA for FY 2019, as amended; and no indicator(s) that the covered individual is a co-author on a publication in an S&E journal with a person(s) on the U.S. BIS Denied Persons List.

Note 1: An indicator may reveal or acknowledge undue foreign influence. Examples include foreign funding or foreign affiliations revealed in proposal disclosures, publications, curriculum vitae (CV), institution website announcements, or social media posts.
Note 2: Participation may be identified by a contract between the covered individual and an MFTRP, reported by the covered individual in the fundamental research project proposal or on a CV or resume, or identified in an acknowledgement in a publication listing the covered individual and an MFTRP.
Note 3: Section 238 of the NDAA for FY 2025 (Public Law 118-159), "Limitation on Availability of Funds for Fundamental Research Collaboration with Certain Academic Institutions." The Assistant Secretary of Defense for Science and Technology may waive this limitation on a case-by-case basis with respect to an individual grant or contract for an institution of higher education if the Assistant Secretary determines that such a waiver is in the national security interests of the United States.
Note 4: "Collaborations for the Specific Purposes of Fundamental Research" means research that is identified in the fundamental research project proposal that is to be conducted with an entity that is included on the most recent version of the list developed pursuant to section 1286 of the NDAA for FY 2019, as amended, or to any employees of such entities.
Note 5: The list of "Institutions of the People's Republic of China, Russian Federation, and Other Countries with Specified Characteristics" developed pursuant to section 1286 of the NDAA for FY 2019, as amended, is published at https://rt.cto.mil/stpp/mta/.
Note 6: The level of mitigation needed is elevated if any of the disclosed or identified indicators occurred after the signing of the CHIPS and Science Act of 2022.
Note 7: An addition to the U.S. BIS Entity List is active on or after the Federal Register citation date provided on the U.S. BIS Entity List.
Note 8: EO 14032, "Addressing the Threat from Securities Investments That Finance Certain Companies of the People's Republic of China," dated 3 Jun 2021 (superseding EO 13959), bans new U.S. investment in certain communist military companies (CCMCs). The DoD maintains and updates lists of CCMCs for the purposes of compliance with EO 14032.
Note 9: Most recent annual version of "The Notice of Designation of Chinese Military Companies" under section 1260H of the NDAA for FY 2021.
Note 10: The need for mitigation is elevated if any of the disclosed or identified indicators occurred after publication of the Under Secretary of Defense for Research and Engineering "Letter to Academia," dated 10 Oct 2019.
Note 11: Co-authorship is identified as a category where mitigation is suggested when a covered individual is collaborating with entities or persons associated with factors listed in this matrix and should not be a basis for rejection of a fundamental research project proposal.
Note 12: Individuals on the U.S. BIS Denied Persons List are active between the effective date and the expiration date provided on the U.S. BIS Denied Persons List.

DARPA FRRBS w/ 2025 Matrix Q&A

- Q1: What is DARPA's timeline for implementing the 2025 Matrix?
  - A1: 2025 Matrix was implemented on 12 May 2025
- Q2: Has there been any communications sent to components requiring them to involve institutional officials and their offices when completing mitigation plans?
  - A2a: Unfortunately, No. Each agency mitigates the risks based on their internal "risk tolerance." DARPA does share mitigation strategies with other agencies (NOT Risk Assessments) when contacted by performer and agency.
  - A2b: DARPA's policy is to include the institutions officials (Vice President / Chancelor of Research and/or Office of Research Security) when initiating negotiations for mitigations. Typically, we do not directly work with the individual of concern; communications are primarily through the Research Security Office and other officials.
- Q3: COGR encouraged DoD during a previous outreach visit involving the BSO, DARPA and ARO to create a template for mitigation plans. While we recognize that each plan will be different, we still believe it's possible to have a shell template that can be used as a starting point. This would be particularly helpful for smaller and less resourced institutions.
  - A3: Ideally, templates would make the process easier. However, each mitigation case is unique and is generally addressed best through memorandum format addressing each individual concern. Supporting attachments are always encouraged (e.g. signed attestations, email disclosures, training records, etc.) to help support the strategy.

DARPA FRRBS w/ 2025 Matrix Q&A (cont)

- Q4: The Risk Review Matrix requires disclosure of patents or patent applications resulting from USG-funded research filed in a country of concern before the U.S. or filed on behalf of an FCOC entity. Several of our members have reported mitigation plans being required for a proposal despite the patent/patent applications in question not pertaining to the proposed research. Can you clarify what is the intended scope for the disclosure of patent/patent applications?
  - A4: The requirement to disclose patent filing stems from the issue of USG / DoD funding research, then that research being patented in a foreign country prior to the U.S. When the USG / DoD funds research it expects to benefit from that research prior to other FCOC entities. The scope of disclosure is for all patents to be disclosed to give a "total picture" of the researcher and how their patent filings have occurred.
- Q5: With greater frequency, federal agencies have used federal restricted party lists to promote US foreign policy. Federal RPS list additions, deletions and updates are generally noticed via the eCFR and picked up automatically through the free consolidated screening list search engine found on Trade.Gov and/or by third party vendors like Descartes Visual Compliance and Amber Road/E2Open. Are there any plans to start posting additions, deletions, or revisions to DOD's 1286 and 1260H lists to the eCFR? This approach would make it much easier for the defense industrial base to know that they are checking against the most recent lists available.
  - A5: OUSD(R&E) is working on a more "living" list that is updated more than annually. The DoD components now have the ability to suggest additions to the 1286 list and the list is updated more frequently. Will follow up with OUSD(R&E) once more information is available. The 1260H list remains an annual updated list.

DARPA FRRBS w/ 2025 Matrix Q&A (cont)

- Q6: From the 2025 Matrix: "Collaborations for the specific purpose of fundamental research[4] between institutions of higher education and academic institutions that are included in the most recently updated list developed pursuant to section 1286 of the NDAA for FY 2019, as amended, or employees of such institutions."

Note 4 states: "Collaborations for the Specific Purposes of Fundamental Research" means research that is identified in the fundamental research project proposal that is to be conducted with an entity that is included on the most recent version of the list developed pursuant to section 1286 of the NDAA for FY 2019, as amended, or to any employees of such entities.

Can DARPA clarify whether the new matrix prohibits any/all collaborations with entities on the 1286 List, or, if as noted in Note 4, this prohibition only applies to collaborations involving the specific fundamental research being proposed under the DoD grant?

- A6: DARPA's interpretation of NOTE 4 on Factor 4 is that this only applies to a specific fundamental research proposal to DARPA that proposes to included a collaborative effort with an entity on the 1286 list. (e.g. as a sub-contractor or conducting program work at a 1286 listed institution).
  - DARPA does not have the ability to identify any/all research an institution is performing in collaboration with entities on the 1286 list unless they are all disclosed in a proposal. Additionally, if it is NOT USG/DoD funded then it is not relevant to our assessment.

www.darpa.mil

Poll Everywhere

Pollev.com/cogrstaff949 Ask a question from your seat!

COGR