CLEAR Meeting

Presented by Sponsored Research | February 11, 2026

Today's Agenda

- Announcements
- Communicating with Sponsored Research
- Budget Revisions Across the Funding Lifecycle
- DoD Cybersecurity Maturity Model Certification (CMMC) Awareness
- SR & IT Security

Advance and At-Risk Requests

- Advance & At-Risk requests no longer require school approvals to be uploaded in CERES!
- Post 'Interim Funding' Revised Automatic Extensions: NIH R and K series delayed continuations will now be automatically extended by SR the month prior to the budget period end date for the next full period of funding
    - Note: All other delayed continuations (other NIH types and other sponsors) will require a formal at-risk request in CERES
    - SR in process of catching up, please allow a couple of weeks for us to do so

Upcoming NIH Due Dates

NIH Due Date	SR (5-Day) Deadline	Description
March 5	February 26	• **R01 Research Grants** • **U01 Research Grants - Cooperative Agreements** *renewal, resubmission, revision*
March 12	March 5	• **K Series Research Career Development** *renewal, resubmission, revision*
March 16	March 9	• **Other Research Grants and Cooperative Agreements** (R03, R21, R33, R21/R33, R34, R36, U34, UH2, UH3, UH2/UH3) *renewal, resubmission, revision*
April 8	April 1	• **F Series Fellowships *Individual* NRSAs** (including F31 Diversity) *new, renewal, resubmission*
April 12* (Sunday)	April 6	• **R13, U13 Conference Grants & Cooperative Agreements** *All - new, renewal, resubmission, revision*

**due date pushes to next business day*

Proposal Deadline Exception Requests

- Approved exception allows SR staff to prioritize review of a late proposal or for science to be submitted outside of 5-day deadline, however **submission is never guaranteed**
- Exceptions can only be approved by SR Asst. Vice President and Director of Pre-AM
- **Rare and extenuating circumstances only!**
- Must use Smartsheet exception form
- Review/approval process:
    1. School Associate Dean of Research
    2. THEN Sponsored Research
- Both approvals needed
- Proposals with a declined exception (at either level) are reviewed in order received

NIH Common Form Leniency Period 🎉

NOT-OD-26-033 & updated FAQs:

- **NIH will allow a period of leniency through May 2026** regarding the use of the Common Forms for Biographical Sketches and Other Support, which are required for application due dates and all JIT, RPPR, and Prior Approval submissions on or after January 25, 2026.
- **During the period of leniency, NIH will not withdraw applications** that don't comply with the use of the Common Forms.
- Use of Common Forms is still **strongly** encouraged.

Resources

- NIHs Implementation of Common Forms for Biographical Sketch and Current and Pending (Other) Support for Due Dates on or after January 25, 2026 (NOT-OD-26-018)
- NIH Biosketch Format Pages, Instructions, and Samples
- Galter Library: NIH Biosketch Guide
- Galter Library: Using SciENcv to Create an NIH Biosketch and Other Support Documents

New & Upcoming SR Events

SR is introducing more opportunities to engage with Sponsored Research:

- **SR Coffee Hour Connect** (online):
  - Virtual How-To Sessions with SR staff
  - Time for Q&A
  - Planned: Navigating CERES for subawards (March TBD); What is the status of an award negotiation; Where is my proposal at in the queue; and more!
- **Meet SR Staff** (in person):
  - Outreach/presentations
  - Post CLEAR team meet & greets (today meet the Pre-Award team!)
- **Webinar Group Watches** (hybrid):
  - Save the Date: March 4, 1:30pm: SRAI Encore Series, "Research Project Management in a Crisis: Navigating Federal Transitions and Uncertainty“

Communicating with Sponsored Research

Cathy Barrera

Communicating with Sponsored Research

Considerations Before you Reach Out

1. Have you reviewed ***all available resources***, including:
   - Sponsored Research Handbook
   - Sponsored Research website & job aids
   - CERES training
   - Northwestern Policies & Guidance
   - Sponsor Resources such as sponsor terms & conditions, the NIH Grants Policy Statement, the NSF PAPPG, etc.

2. Have you ***consulted with department colleagues and school/department leadership?***

Tip: Subscribe to the ***NURAP Link Up Teams Channel*** for other resources and announcements

Who Should you Contact?

Pre-Award

- Proposals
- Post submission updates
- Just-in-time

Award Management

- Award modification requests
- Progress reports/RPPRs (anticipated January 2026)
- Amendments w/o term and condition changes
- Overdue reports compliance
- Advance and at-risk requests

Contracts & Award Acceptance

- Award reviews
- Negotiations
- Non-funded agreements
- Amendments w/ term & condition modifications
- Clinical trials (awards & amendments)
- Proposal redlines
- FOIA requests

Subcontracts Management

- Outgoing subaward agreements
- Outgoing subaward amendments
- Outgoing subaward related award modification requests

Business Systems & Operations

- Award setup
- Post-award request processing
- CERES functional support
- Grant submission system access
- Patent/invention reporting
- Reporting/data analytics
- Internal workflow coordination

Who Should you Contact?

Reason for Reaching Out	Who to Contact
Question on specific award or proposal	Specialist listed on the CERES FP or AWD
Question on policy, complex issue, or escalation	SR Leadership
Technical question (CERES, Commons IDs, etc.)	Business Systems & Operations Team via osr-info@northwestern.edu
New award notice/letter	Send to SponsoredResearch@northwestern.edu for identification, log in, and assignment
Status of an award review or agreement negotiation	“Owner” listed on the SRA / CTA in CERES
Status of an outgoing subcontract	“Owner” listed on the Outgoing Subaward Agreement in CERES

Communication Requests

- Include the CERES record #, this allows us to quickly (and accurately!) link the request to the correct proposal or award
- Ask questions *within* CERES so communications stay with the record
- SR does not need to be included on internal messages between the department and a PI
- Encourage faculty to reach out to the department with questions first so you can determine whether SR involvement is really needed

Extra Tips for Communication with the Pre-Award Team

- Use the CERES history tab to summarize any unusual circumstances or requirements
- Comments do not send an alert to the SR reviewer
- Clearly communicate midday deadlines
    - Include midday deadline time in title
    - Deadlines before noon list due date of the day before
- Keep communication ***within CERES*** for transparency and coordination should the proposal need to be reassigned to another team member
- Create and use a CERES record for any proposal you have a question on to help document and avoid confusion
- Please do not ask for status updates on a proposal that has been with SR less than 2 business days

Budget Revisions Across the Funding Lifecycle

Award Management Team
Maggie Hays
Mary Rosenthal
Anna Roth

Budget Revisons

There are many reasons why a proposed budget may need to be updated or changed at various points in the funding lifecycle.

This includes:

- **Pre-Award** revisions
- **Post-Award** budgets provided as part of a progress report or to trigger an anticipated outyear
- **Post-Award** revisions needed to align with changes in project scope, personnel, etc.

Reminders

All budgets submitted to a sponsor require ***institutional review and endorsement*** prior to submission.

You may provide draft revisions to a sponsor for feedback, but all changes must be ***clearly documented in CERES*** to avoid delays or confusion at award setup.

All proposed changes must conform to ***Northwestern and sponsor policies*** and meet the Uniform Guidance cost principles (e.g. costs must be allowable, allocable, reasonable, and consistently applied.)

Pre-Award Revisions

At **Just-in-Time** stage, a sponsor may require a revised budget based on the recommended funding and/or to remove unallowable costs.

If you receive such a request, use the **Proposal Status Confirmation** activity in CERES to alert SR. We can then open the CERES record for revision.

*Note, this is not required when a sponsor makes minor, unilateral reductions to an award; the Award Set Up team can capture any changes via **budget reconciliation**.*

Pre-Award Revisions

FULL REVISION
OR
ANNUAL REVISION?

Consider whether you can rebudget for the **full project period** (e.g. Y1-5) or if it has to be done on an **annual/per period** basis (Y1 only).

The latter would require annual AMRs if the outyear amounts are uncertain.

Annual Revisions

When sponsors, including pass-through-entities, require submission of a budget with each **progress report**:

- These receive a standard review as part of the Continuation record
- SR will confirm cost allowability and correct application of rates
- Department should explain any significant changes from the original budget

Note, a separate AMR is not required if the changes are captured in the progress report record in CERES.

Post-Award Revisions

During the life of the award, **changes to the project** may necessitate changes to the budget.

This may occur if:

- A sponsor reduces the budget in an outyear
- There is a change in scope that also requires a budget revision (e.g., adding a subaward, large equipment purchase, etc.)
- A sponsor has other rebudgeting restrictions or thresholds

Be sure to review the award terms and conditions to ensure the sponsor's prior approval is sought when needed.

Increases in Funding

If a sponsor wishes to **supplement** the existing award by providing additional funding (and possibly time), a **Revision** record is needed.

Continuation records do not have a budget module and therefore cannot be used to capture new funding.

CONTINUATION

- Progress Report
- No new $

REVISION

- Supplement
- New $

Award Modification Requests (AMRs)

When is an AMR needed?

- Any time a budget is presented to a sponsor (including a PTE) that is not being reviewed via JIT or the RPPR.
- Any time prior approval is needed (such as for internal reallocations or to add a new cost).
- Any time there is an overall budget reduction of 20% or more, to fully evaluate the impact on the project scope.

*Note, revisions that impact key personnel effort **should also be marked as a Personnel/Effort change** and may require sponsor approval even if the overall budget changes do not.*

Award Modification Requests (AMRs)

When is an AMR NOT needed?

- For **internal reallocation** to cover line-item variances.
- To propose **new funding** (this would require a Revision record.)
- To reflect changes in institutional **base salary or fringe/F&A** rates.
- When an **annual rebudget** is reviewed via an **RPPR Continuation** record.
- For **deobligations**.
- For **spending plans** that do not propose changes to a project but instead discuss how an unobligated balance will be spent down.

AMR Smart Form and Required Information

Is this related to rebudgeting approved carry forward?	If yes, SR needs to know *where* to move the restricted funds.
Are there rebudgeting restrictions indicated in the T&C?	Review the *NOA and related documents* (PAPPG, etc.) to confirm.
Is Sponsor's prior approval required?	If approval is needed, prepare all required information in *sponsor-ready* format. If approval has already been obtained, upload confirmation.
Select all chartstrings involved in the rebudgeting	Include a detailed summary of movement across budget categories and between chartstrings.
Provide any other relevant notes	Provide a brief summary of the changes, and/or communication or instructions from sponsor, etc.

AMR Reminders

1) Check for **COI and RST compliance** (SR must certify when submitting via Research.gov or Commons.)

2) Confirm **IRB or IACUC approvals** are current and linked in CERES.

3) Upload all **required documentation**:

   a. Sponsor communication

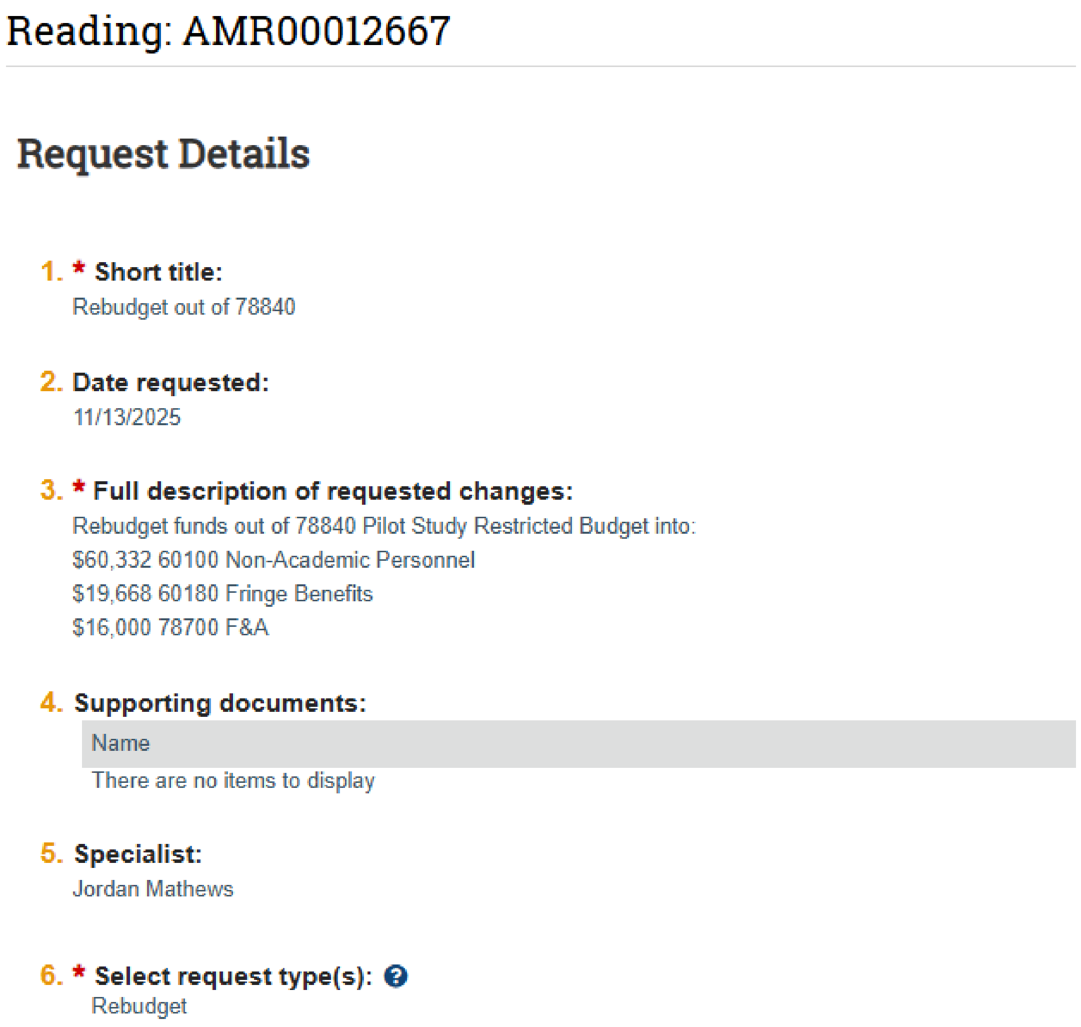
   b. Detailed budget/Reallocation

   c. Budget justification

   d. Amended scope of work, as applicable

   e. Rationale for the request (including applicable thresholds/rebudgeting restrictions)

Sample Rebudget AMR



Reading: AMR00012667

Request Details

1. * **Short title:**
   Rebudget out of 78840

2. **Date requested:**
   11/13/2025

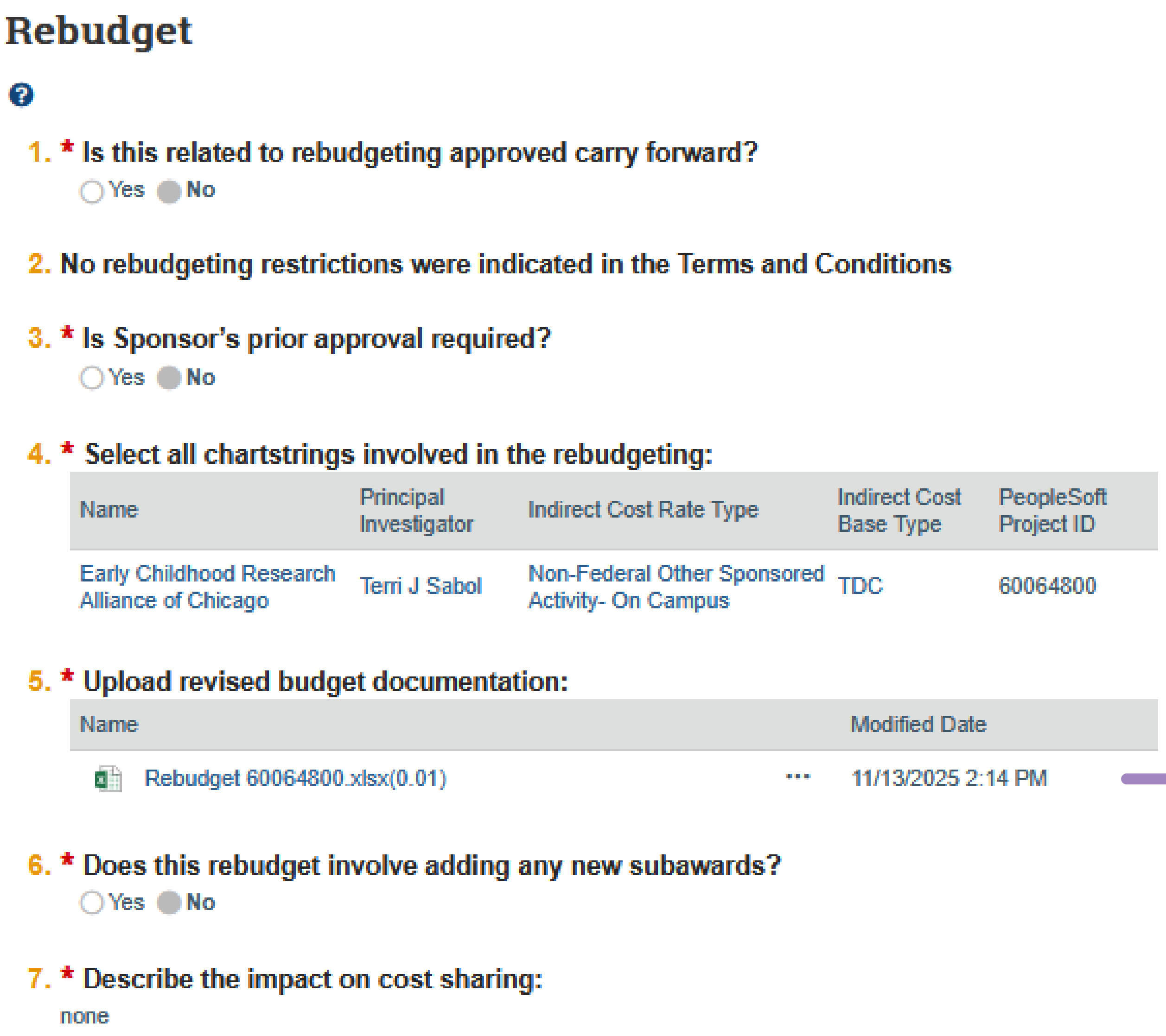
3. * **Full description of requested changes:**
   Rebudget funds out of 78840 Pilot Study Restricted Budget into:
   $60,332 60100 Non-Academic Personnel
   $19,668 60180 Fringe Benefits
   $16,000 78700 F&A

4. **Supporting documents:**

Name
There are no items to display

5. **Specialist:**
   Jordan Mathews

6. * **Select request type(s):** ?
   Rebudget



Rebudget

1. * Is this related to rebudgeting approved carry forward?
   ○ Yes ● No

2. No rebudgeting restrictions were indicated in the Terms and Conditions

3. * Is Sponsor's prior approval required?
   ○ Yes ● No

4. * Select all chartstrings involved in the rebudgeting:

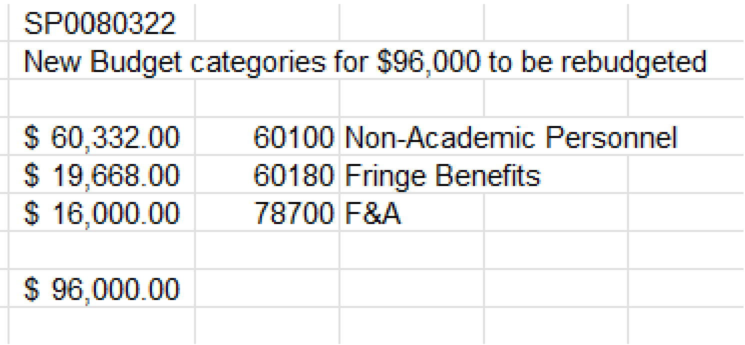
Name	Principal Investigator	Indirect Cost Rate Type	Indirect Cost Base Type	PeopleSoft Project ID
Early Childhood Research Alliance of Chicago	Terri J Sabol	Non-Federal Other Sponsored Activity- On Campus	TDC	60064800

5. * Upload revised budget documentation:

Name		Modified Date
Rebudget 60064800.xlsx(0.01)	•••	11/13/2025 2:14 PM

6. * Does this rebudget involve adding any new subawards?
   ○ Yes ● No

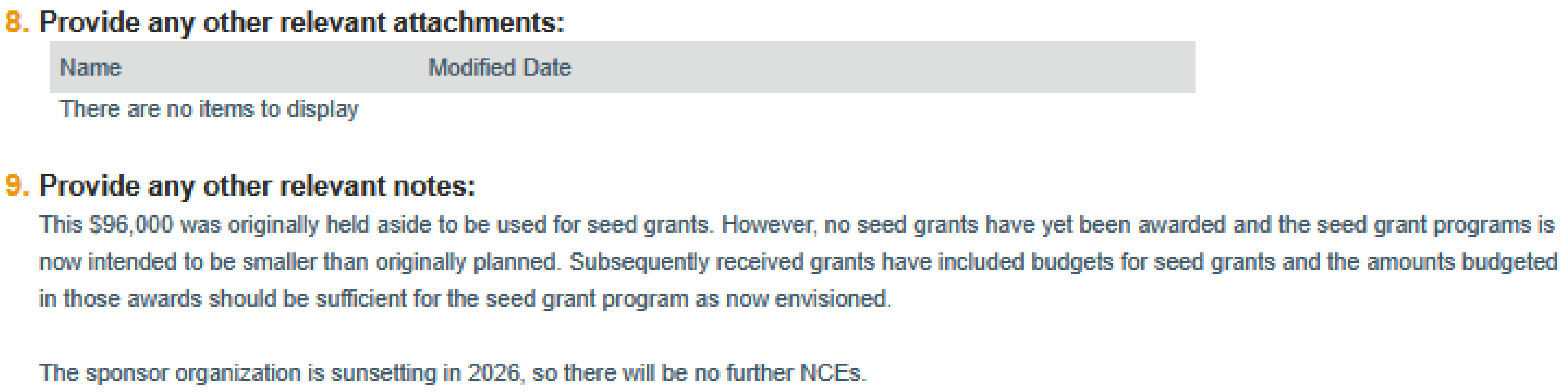
7. * Describe the impact on cost sharing:
   none



SP0080322

New Budget categories for $96,000 to be rebudgeted

$ 60,332.00	60100	Non-Academic Personnel
$ 19,668.00	60180	Fringe Benefits
$ 16,000.00	78700	F&A
$ 96,000.00		



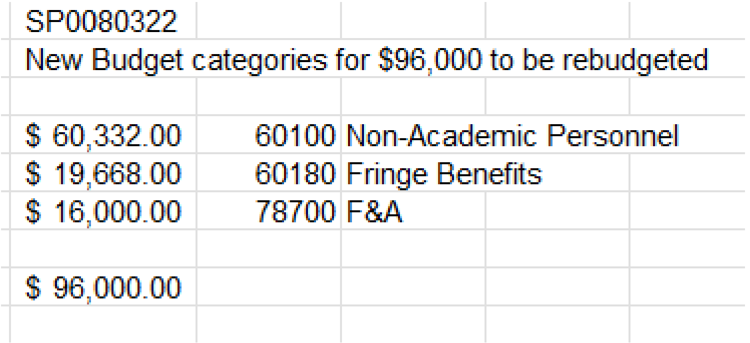
8. Provide any other relevant attachments:

Name	Modified Date
There are no items to display	

9. Provide any other relevant notes:

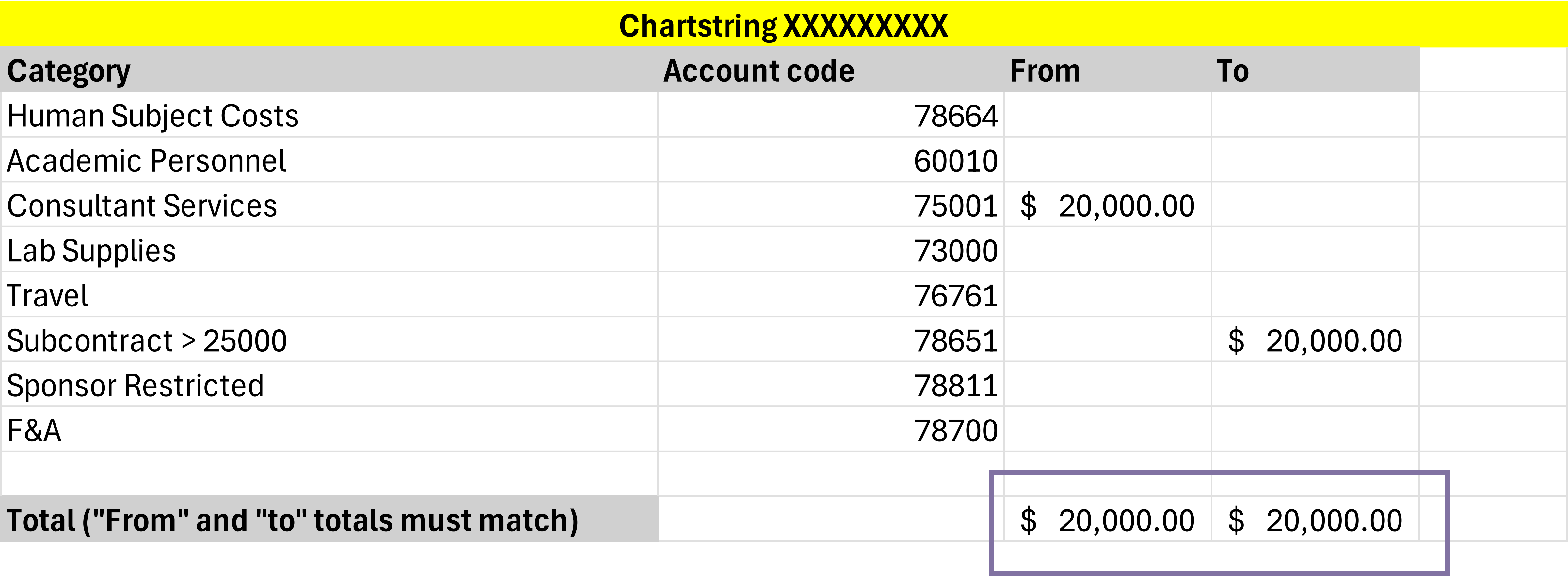
This $96,000 was originally held aside to be used for seed grants. However, no seed grants have yet been awarded and the seed grant programs is now intended to be smaller than originally planned. Subsequently received grants have included budgets for seed grants and the amounts budgeted in those awards should be sufficient for the seed grant program as now envisioned.

The sponsor organization is sunsetting in 2026, so there will be no further NCEs.



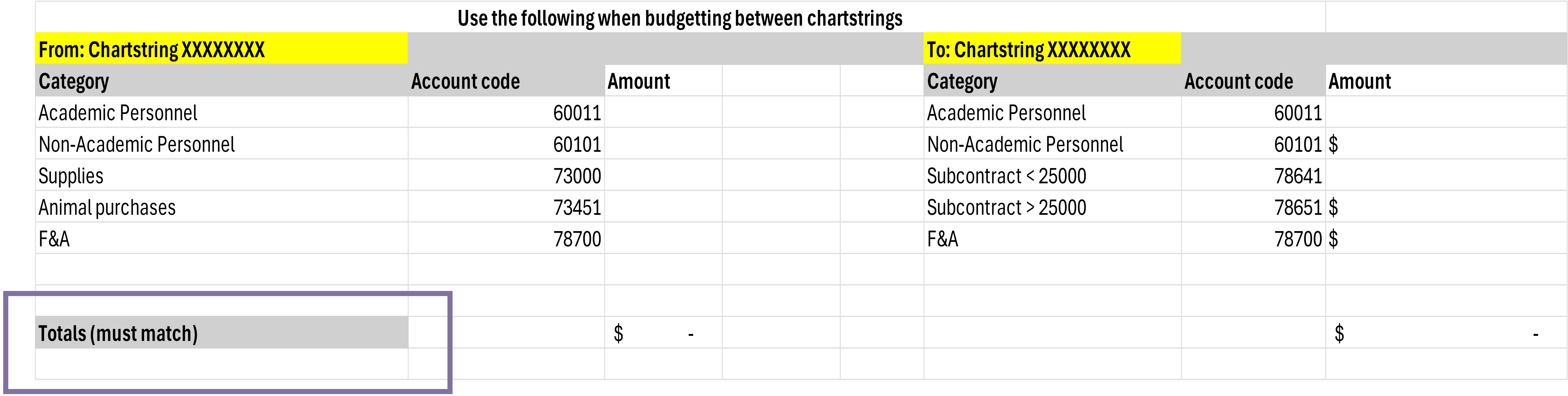
SP0080322		
New Budget categories for $96,000 to be rebudgeted		
$ 60,332.00	60100	Non-Academic Personnel
$ 19,668.00	60180	Fringe Benefits
$ 16,000.00	78700	F&A
$ 96,000.00		

Sample for rebudget with one chart string

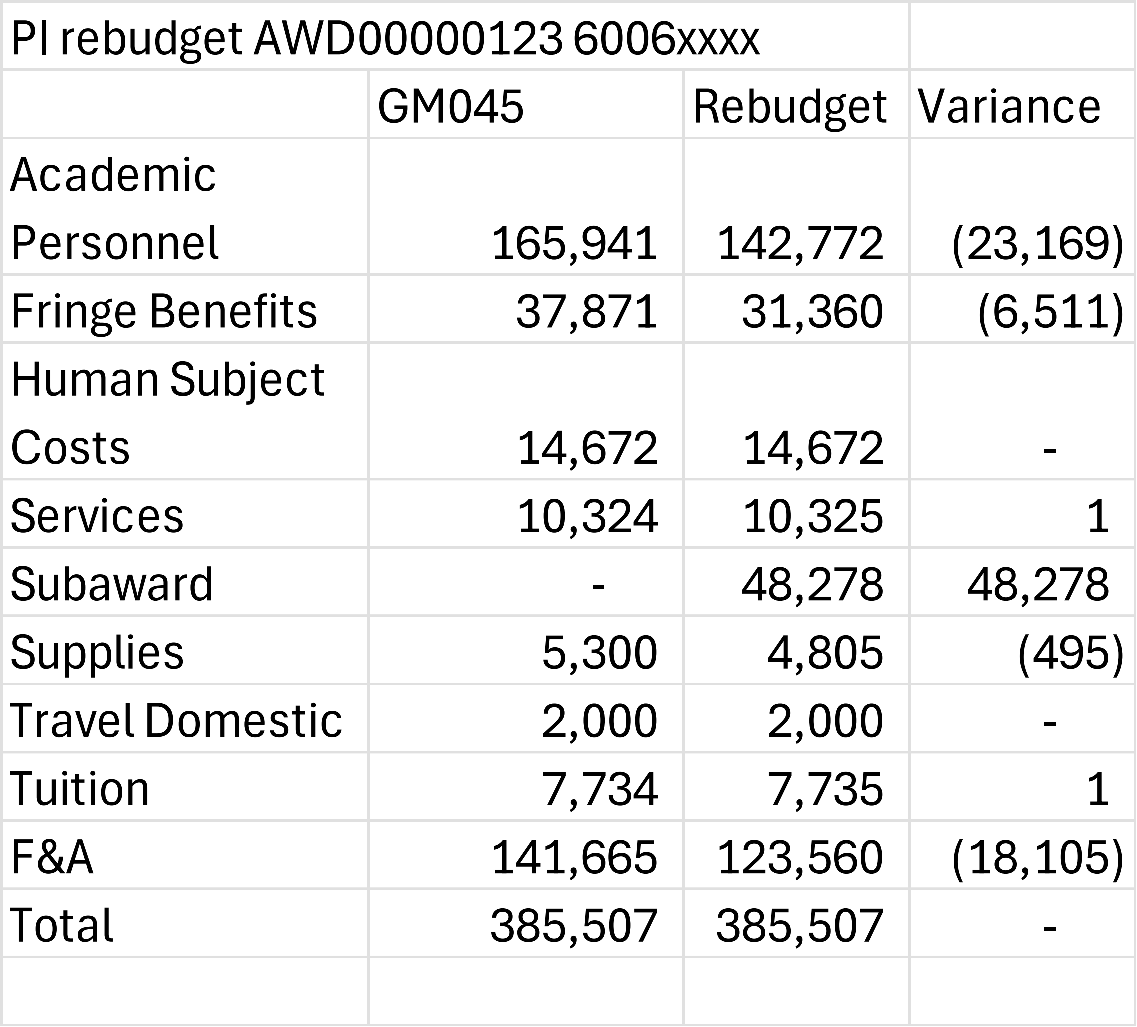


Chartstring XXXXXXXXX			
Category	**Account code**	**From**	**To**
Human Subject Costs	78664		
Academic Personnel	60010		
Consultant Services	75001	$ 20,000.00	
Lab Supplies	73000		
Travel	76761		
Subcontract > 25000	78651		$ 20,000.00
Sponsor Restricted	78811		
F&A	78700		
Total ("From" and "to" totals must match)		$ 20,000.00	$ 20,000.00

Sample for rebudget with multiple chart strings



Use the following when budgetting between chartstrings							
From: Chartstring XXXXXXXX					To: Chartstring XXXXXXXX		
Category	Account code	Amount			Category	Account code	Amount
Academic Personnel	60011				Academic Personnel	60011	
Non-Academic Personnel	60101				Non-Academic Personnel	60101	$
Supplies	73000				Subcontract < 25000	78641	
Animal purchases	73451				Subcontract > 25000	78651	$
F&A	78700				F&A	78700	$
Totals (must match)		$ -					$ -



PI rebudget AWD00000123 6006xxxx			
	GM045	Rebudget	Variance
Academic Personnel	165,941	142,772	(23,169)
Fringe Benefits	37,871	31,360	(6,511)
Human Subject Costs	14,672	14,672	-
Services	10,324	10,325	1
Subaward	-	48,278	48,278
Supplies	5,300	4,805	(495)
Travel Domestic	2,000	2,000	-
Tuition	7,734	7,735	1
F&A	141,665	123,560	(18,105)
Total	385,507	385,507	-

Tips for successful AMRs

- Use a short **descriptive** title.
- **Label attachments clearly** and add dates, if needed, to avoid confusion.
- **Summarize** what is changing and why (justification).
- Be sure to consider the effect on **F&A** for items like subcontracts, tuition, and equipment.
- Do any of the changes necessitate another **AMR** type? (e.g., a subaward amendment, personnel/effort change, or scope change).
- Adding comments does not send SR a notification; it’s preferable to send an **email** via the award in CERES.

Questions?

Carrie Holbo, Director, Pre-Award & Award Management
carrie.holbo@northwestern.edu

Maura Cleffi, Assistant Director, Award Management
m-cleffi@northwestern.edu

DoD Cybersecurity Maturity Model Certification (CMMC) Awareness

Brandon Grill
Northwestern Information Technology
bgrill@northwestern.edu

Agenda

- Background and policy drivers behind CMMC
- CMMC 2.0 structure (levels, assessments, attestations)
- CMMC Implementation at Northwestern
- DFARS clauses identifying where CMMC is implemented
- CMMC in solicitations and what offerors must submit
- Impacts for Northwestern research
- Other 800-171 items and future items to watch

Why CMMC Exists

In short: greater protection and accountability for non-public DoD information

- Defense industrial base highly dependent on self-attestation; audits generally demonstrated significant non-compliance
- Noncompliance due to both lack of standardization as well as audit processes

Enter: CMMC

- Moves the DIB away from pure self-attestation toward verified implementation and sustained compliance
- Standardizes expectations across primes and subcontractors via contract language and a defined assessment ecosystem

High-level CMMC Timeline

- **CUI Program Initiation**
    - Executive Order 13556 in 2010 launched the Controlled Unclassified Information program to unify information protection standards.
- **DoD Cybersecurity Requirements**
    - DFARS 252.204-7012 mandated safeguarding defense information and cyber incident reporting within acquisition frameworks.
- **CMMC Framework Launch**
    - CMMC was announced in 2019 to enhance cybersecurity readiness through third-party validations and maturity levels.
- **Policy Finalization and Enforcement**
    - 2024 and 2025 rules formalized certification ecosystem and contractual enforcement for CMMC compliance in DoD contracts.
    - Phased rollout began November 2025 (Phase 1: Levels 1 & 2 self-assessment); full implementation over ~3 years
    - ***Applies to all DoD contracts involving FCI or CUI, including mandatory flow-down to subcontractors***

Two rules: Program vs Acquisition

Program Rule (32 CFR Part 170)

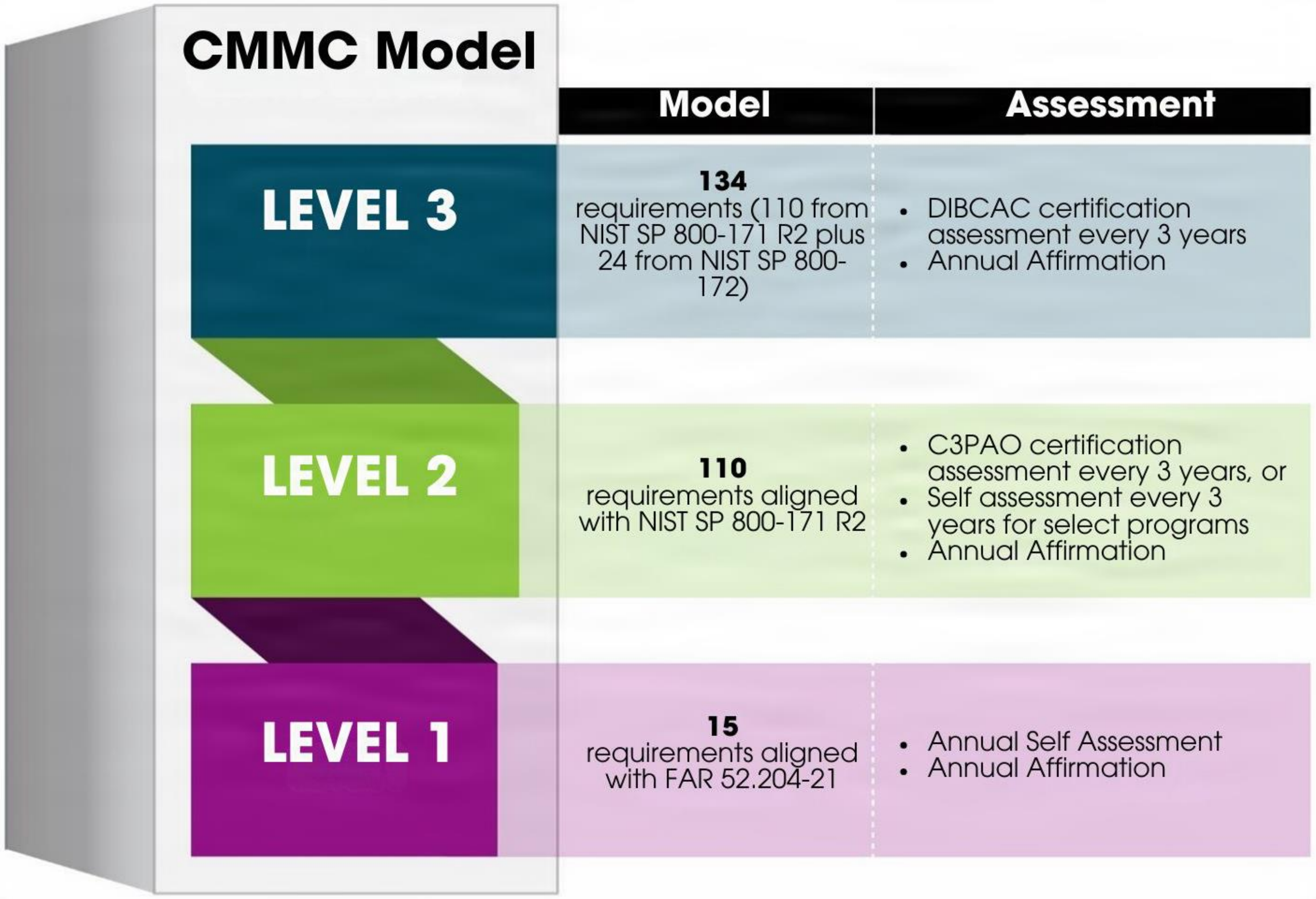
- Defines CMMC levels, assessment types, status, etc.
- Sets applicability and phased implementation
- Defines contractor/subcontractor responsibility

Acquisition Rule (DFARS – 48 CFR)

- Implements CMMC via DFARS policy (Subpart 204.75)
- Creates solicitation provision 252.204-7025
- Updates contract clause 252.204-7021

CMMC Structure – Three Tiers of Certification

- **Level 1: Basic Safeguarding**
  - Protects FCI
  - Safeguarding aligned to FAR 52.204-21 baseline
- **Level 2: Controlled Unclassified Information**
  - Protects CUI
  - Aligned to NIST SP 800-171 Rev. 2
  - *Northwestern (generally) does not currently accept CUI due to restrictions that conflict with fundamental research ore export controls*
- **Level 3: Enhanced Security Controls**
  - “High Priority” CUI
  - Adds selected NIST SP 800-172 requirements



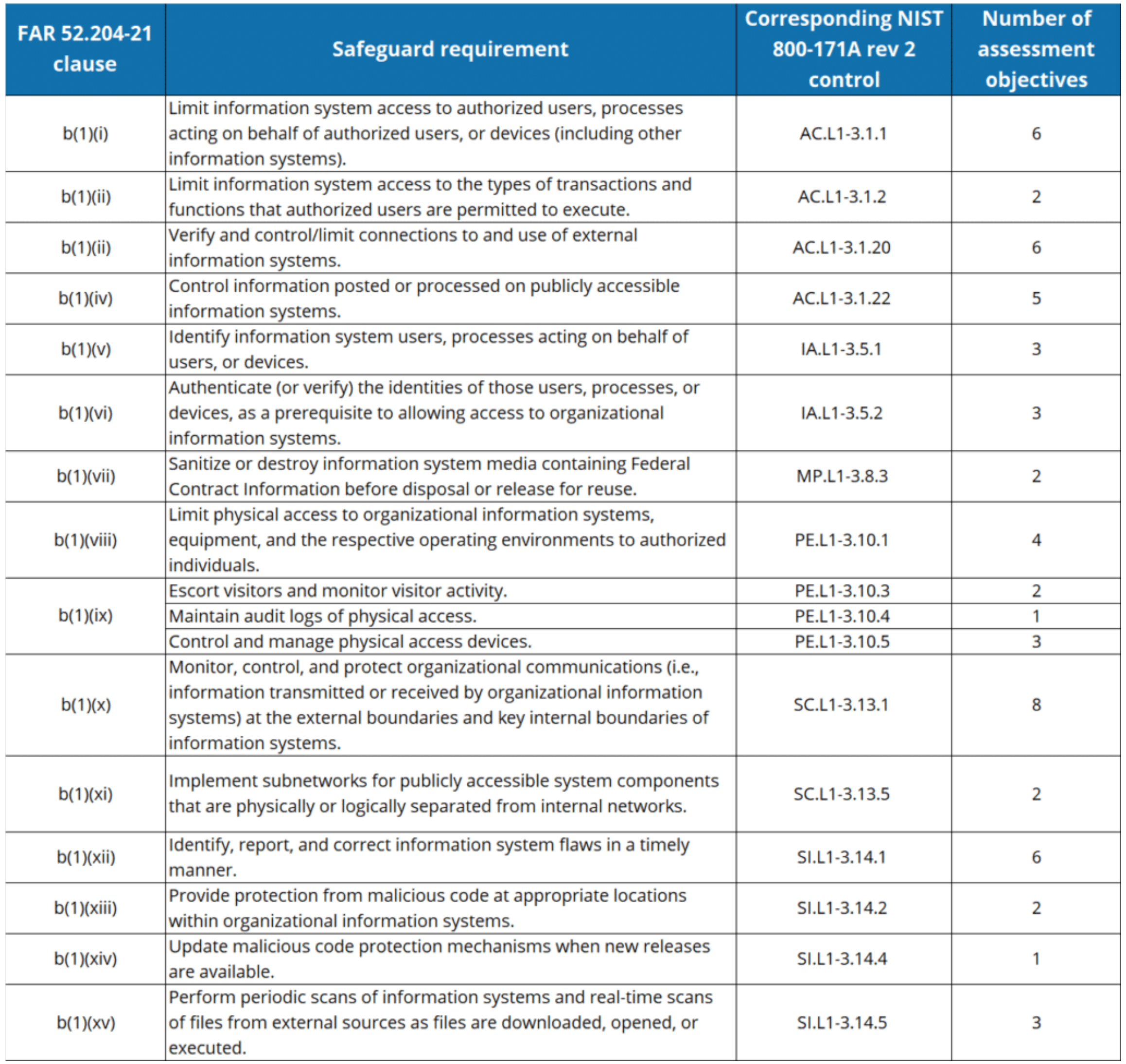
CMMC Model

	Model	Assessment
LEVEL 3	**134** requirements (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172)	• DIBCAC certification assessment every 3 years • Annual Affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171 R2	• C3PAO certification assessment every 3 years, or • Self assessment every 3 years for select programs • Annual Affirmation
LEVEL 1	**15** requirements aligned with FAR 52.204-21	• Annual Self Assessment • Annual Affirmation

CMMC 2.0 Implementation at Northwestern

- Pre-Award: determine what is FCI/CUI ***this is the hardest part***
- Level 1: Collection of managed technologies (Managed endpoints, RDSS-Audit, M365)
  - Documentation completed and preparing for certification
  - Shared responsibility matrix with PIs
- Level 2: Identification of managed service providers and paths forward
  - General compute and productivity
  - High-performance computing
  - Laboratories (non-data) projects will require significant additional effort
  - Need to coordinate export control and other potential restrictions
- Level 3: Not currently planned

CMMC Level 1

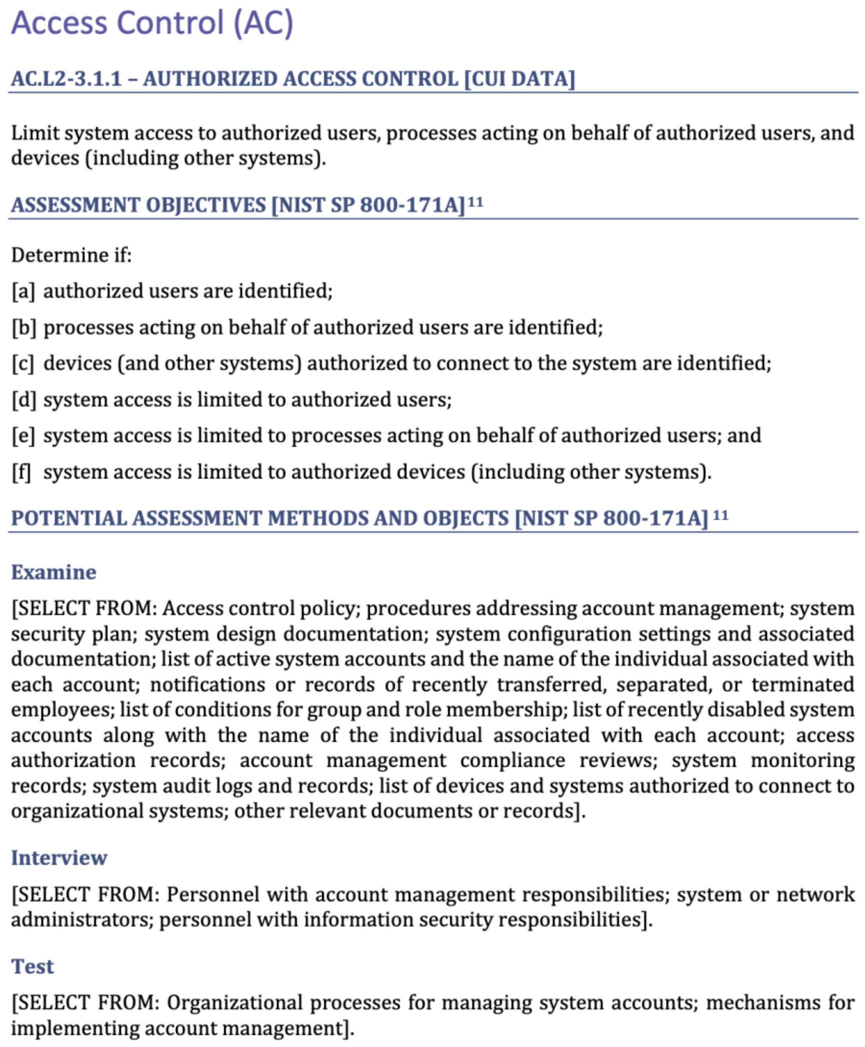


FAR 52.204-21 clause	Safeguard requirement	Corresponding NIST 800-171A rev 2 control	Number of assessment objectives
b(1)(i)	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	AC.L1-3.1.1	6
b(1)(ii)	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	AC.L1-3.1.2	2
b(1)(ii)	Verify and control/limit connections to and use of external information systems.	AC.L1-3.1.20	6
b(1)(iv)	Control information posted or processed on publicly accessible information systems.	AC.L1-3.1.22	5
b(1)(v)	Identify information system users, processes acting on behalf of users, or devices.	IA.L1-3.5.1	3
b(1)(vi)	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	IA.L1-3.5.2	3
b(1)(vii)	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	MP.L1-3.8.3	2
b(1)(viii)	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	PE.L1-3.10.1	4
b(1)(ix)	Escort visitors and monitor visitor activity.	PE.L1-3.10.3	2
	Maintain audit logs of physical access.	PE.L1-3.10.4	1
	Control and manage physical access devices.	PE.L1-3.10.5	3
b(1)(x)	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 information systems.	SC.L1-3.13.1	8
b(1)(xi)	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	SC.L1-3.13.5	2
b(1)(xii)	Identify, report, and correct information system flaws in a timely manner.	SI.L1-3.14.1	6
b(1)(xiii)	Provide protection from malicious code at appropriate locations within organizational information systems.	SI.L1-3.14.2	2
b(1)(xiv)	Update malicious code protection mechanisms when new releases are available.	SI.L1-3.14.4	1
b(1)(xv)	Perform periodic scans of information systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	SI.L1-3.14.5	3

Self-Assessment Process

To fully implement a control, there must be:

1. A documented policy for each control
2. Processes, procedures, and/or technology implanted to enforce that policy, and
3. A method to check (audit) that the process, procedure and/or technology is working



Access Control (AC)

AC.L2-3.1.1 – AUTHORIZED ACCESS CONTROL [CUI DATA]

Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A][11]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A][11]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

Interview

[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

CMMC Level 1 – Shared Responsibility

Area	Responsibility
Access Control	Only access FCI that I am authorized to view and that is necessary for my official duties. Do not share FCI with unauthorized individuals.
Workstation Security	Lock workstations when unattended and ensure that FCI is not viewable by unauthorized persons.
Data Storage	Ensure FCI is only stored in approved CMMC Level 1 systems. If there is a need to access FCI in any other manner or form (e.g., hard copy, thumb drives, etc.) contact the Information Security Office for guidance.
Transmission	Transmit FCI only through approved encrypted channels (e.g., encrypted email, secure file transfer). Never send FCI over unencrypted or public channels.
Printing and Disposal	Do not print FCI unless approved in advanced, follow all approved FCI documentation handling procedures. FCI is only to be maintained in approved CMMC Level 1 environments.
Email and Collaboration Tools	Do not forward or upload FCI to public or non-approved platforms (e.g., personal email, cloud drives) and will follow University-approved workflows for sharing FCI.
Incident Reporting	Immediately report any security incident, data breach, or unauthorized disclosure involving FCI to the PI and the Office of Information Security immediately per Northwestern's Incident Response Protocol.
Mobile Devices	Do not use mobile devices unless approved in advance, and these devices encrypted, password-protected, and managed by the University's mobile device management (MDM) system.
Removable Media	D not use removable media (USB drives, CDs, etc.) for FCI unless authorized in advance, and these media have required data protection controls (e.g., encrypted).
Personnel and Physical Security	Ensure physical areas where I am processing FCI is secure and that people not authorized to access FCI cannot view or access FCI inadvertently, by overhearing conversations, able to view your screen, etc.

DFARS Clauses: Where to find CMMC

252.204-7012

- The original – required safeguarding of “covered defense information” and cyber incident reporting (baseline obligations)

252.204-7020

- NIST SP 800-171 DoD Assessment Requirements (also pre-dates CMMC)

252.204-7021

- **Contract clause**: maintain required CMMC level/status during performance of contract; defines “current” and ”status” logic

252.204-7025

- **Solicitation provision**: Tells offerors required level; eligibility gates; requires CMMC UID(s) in proposal

CMMC <> Research at Northwestern

- Determination of FCI/CUI. If the project does not store, process, generate, or transmit these data, CMMC may not apply. ****This is the most difficult part****
- If the award mentions CUI or DFARS clauses like 252.204-7012/7021/7025, it is likely that a CUI environment will need to be used
- Expect ”gates” at proposal stage:
  - Solicitations require a CMMC status in SPRS *before award or submission*
  - System details on where work will be performed (e.g. CMMC UID)
- Expect more restrictions on where/how research can take place and/or higher costs of research
  - Personally owned vs. university-owned computers
  - Systems or applications specifically authorized for CMMC research
  - Higher shared costs of using compliant environments
  - More steps or possible restrictions on collaborations
  - Higher administrative burden

More Fun with 800-171

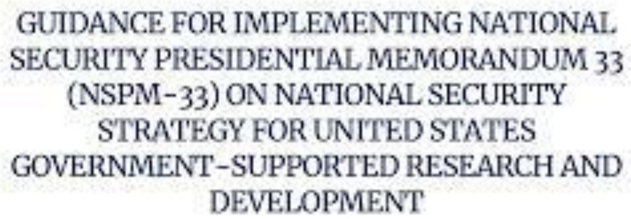
NIH Controlled Access Datasets

- Starting ~13 months ago – data from NIH Controlled Access Repositories(e.g. dbGaP) requires protection to NIST 800-171 *but is not considered CUI*.
- Solutions include Google Cloud Secure Enclave and Nightingale@NU

State and Local Government, Private Companies

- City/state agreements often will reference NIST 800-53
- Negotiation generally align on NIST 800-171, even if the data are not CUI.
- Solutions include Google Cloud Secure Enclave and Nightingale@NU

Watchlist: NSPM-33



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

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NIST Interagency Report 8481

Cybersecurity for Research: Findings and Possible Paths Forward

EDUCAUSE

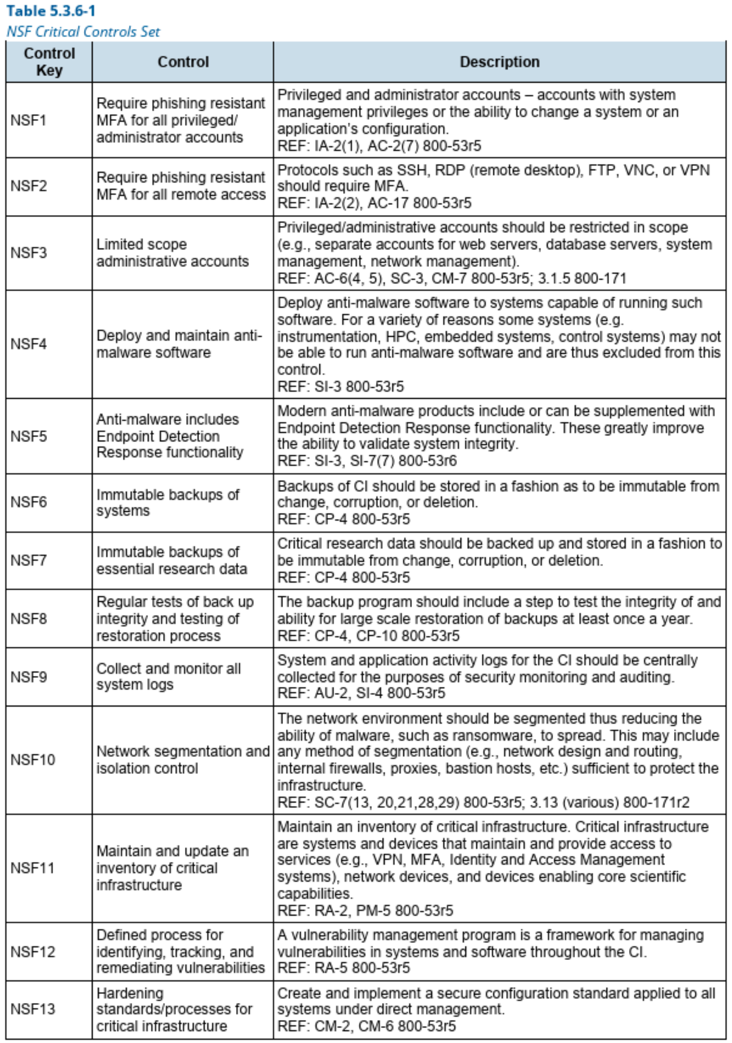


Table 5.3.6-1

NSF Critical Controls Set

Control Key	Control	Description
NSF1	Require phishing resistant MFA for all privileged/ administrator accounts	Privileged and administrator accounts – accounts with system management privileges or the ability to change a system or an application's configuration. REF: IA-2(1), AC-2(7) 800-53r5
NSF2	Require phishing resistant MFA for all remote access	Protocols such as SSH, RDP (remote desktop), FTP, VNC, or VPN should require MFA. REF: IA-2(2), AC-17 800-53r5
NSF3	Limited scope administrative accounts	Privileged/administrative accounts should be restricted in scope (e.g., separate accounts for web servers, database servers, system management, network management). REF: AC-6(4, 5), SC-3, CM-7 800-53r5; 3.1.5 800-171
NSF4	Deploy and maintain anti-malware software	Deploy anti-malware software to systems capable of running such software. For a variety of reasons some systems (e.g. instrumentation, HPC, embedded systems, control systems) may not be able to run anti-malware software and are thus excluded from this control. REF: SI-3 800-53r5
NSF5	Anti-malware includes Endpoint Detection Response functionality	Modern anti-malware products include or can be supplemented with Endpoint Detection Response functionality. These greatly improve the ability to validate system integrity. REF: SI-3, SI-7(7) 800-53r6
NSF6	Immutable backups of systems	Backups of CI should be stored in a fashion as to be immutable from change, corruption, or deletion. REF: CP-4 800-53r5
NSF7	Immutable backups of essential research data	Critical research data should be backed up and stored in a fashion to be immutable from change, corruption, or deletion. REF: CP-4 800-53r5
NSF8	Regular tests of back up integrity and testing of restoration process	The backup program should include a step to test the integrity of and ability for large scale restoration of backups at least once a year. REF: CP-4, CP-10 800-53r5
NSF9	Collect and monitor all system logs	System and application activity logs for the CI should be centrally collected for the purposes of security monitoring and auditing. REF: AU-2, SI-4 800-53r5
NSF10	Network segmentation and isolation control	The network environment should be segmented thus reducing the ability of malware, such as ransomware, to spread. This may include any method of segmentation (e.g., network design and routing, internal firewalls, proxies, bastion hosts, etc.) sufficient to protect the infrastructure. REF: SC-7(13, 20,21,28,29) 800-53r5; 3.13 (various) 800-171r2
NSF11	Maintain and update an inventory of critical infrastructure	Maintain an inventory of critical infrastructure. Critical infrastructure are systems and devices that maintain and provide access to services (e.g., VPN, MFA, Identity and Access Management systems), network devices, and devices enabling core scientific capabilities. REF: RA-2, PM-5 800-53r5
NSF12	Defined process for identifying, tracking, and remediating vulnerabilities	A vulnerability management program is a framework for managing vulnerabilities in systems and software throughout the CI. REF: RA-5 800-53r5
NSF13	Hardening standards/processes for critical infrastructure	Create and implement a secure configuration standard applied to all systems under direct management. REF: CM-2, CM-6 800-53r5

Questions?

Sponsored Research and IT Security

Clay Arnett

How SR Interacts with IT Security

- **Issue Identification**
  SR reviews award documents and proposals and identifies any IT security requirements or concerns.
- **Escalation & Review**
  SR notifies IT Security by initiating an ancillary review in CERES or sends an email.
- **Coordination & Resolution**
  SR collaborates with IT Security and the department/school IT team to address the security requirements.
- **Implementation**
  IT Security and/or department/school IT work directly with the PI to establish an appropriate workspace with the required level of security.

Thank you for attending!

Idea for future CLEAR meeting or ‘SR Coffee Hour Connect’?
Send to c-barrera@northwestern.edu or mmizwa@northwestern.edu