Research Administration Network Agenda

SUB Lobo A&B

## July 11th, 2017

9:00am to 10:00am

1. Introductions

2. Presentations

   - Jeff Gassaway, Information Security & Privacy Office
     Topic: Improving Information Security Practices at UNM

   - Jeremy Hamlin, Contract & Gant Accounting
     Topic: Updating the Master PI Org Code schedule

3. Pre Award items

   - Cayuse Upgrade to 3.6

   - Updates to Cayuse routing

4. Post Award items

   - New process for collection of ABS

5. Upcoming training

6. Reminders

7. Closing remarks

Government

E.O. 13556

Registry

32 CFR 2002

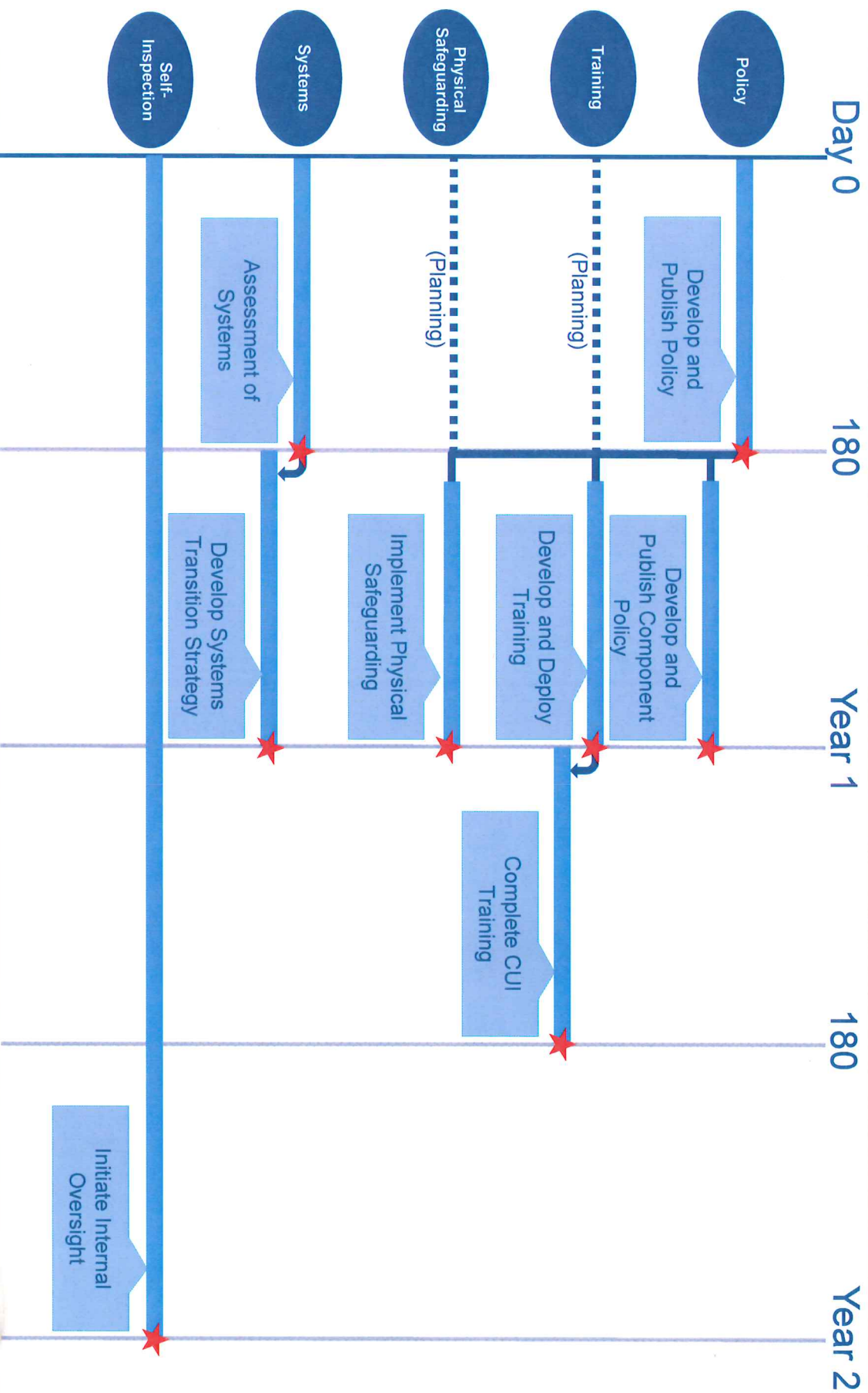NIST SP 800-171

FAR
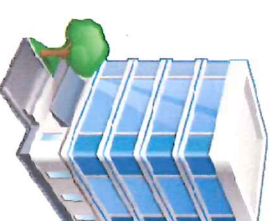
1 Year

Industry

Until the formal process of establishing a single FAR clause takes place, the CUI requirements in NIST SP 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.

The Department of Defense has revised its DFARS to reference the NIST SP 800-171.

CONTROLLED
UNCLASSIFIED
INFORMATION

Implementation of the CUI Program

Timeline phases: Policy, Training, Physical Safeguarding, Systems, Self-Inspection

Timeline markers: Day 0, 180, Year 1, 180, Year 2

Policy:
- Develop and Publish Policy
- Develop and Publish Component Policy

Training:
- (Planning)
- Develop and Deploy Training
- Complete CUI Training

Physical Safeguarding:
- (Planning)
- Implement Physical Safeguarding

Systems:
- Assessment of Systems
- Develop Systems Transition Strategy

Self-Inspection:
- Initiate Internal Oversight

CONTROLLED UNCLASSIFIED INFORMATION

Proposal for Addressing UNM Controlled Unclassified Information (CUI)

In accordance with Federal regulatory requirements as described in Executive Order 13556; 32CFR2002; NIST SP 800-171; FAR, UNM will be required to comply with these regulations for the collection, storage, processing, and/ or transmission of CUI information and systems.

The initial effort to work toward compliance should include the following:
- Inventory of the information that is classified as CUI, including its locations and whether it is in paper or in electronic forms.
- Document of the CUI information and systems safeguards to determine whether there are potential compliance gaps.
- Review, and if needed, update of UNM's Information Security Program, to bring it into accord with CUI requirements.
- Review, and if needed, update UNM's information security & privacy training, to bring it into accord with CUI requirements.
- Review, and if needed, update other relevant policies and data classification.

The initial team steering this effort consist of:
- Chief Compliance Officer
- Facility Security Officer
- Information Security & Privacy Officer
- Office of the Vice President for Research
- HR Data Steward
- FERPA Data Steward
- Financial Aid Data Steward
- Finance Data Steward

Once this initial effort is complete, it is recommended that a report of the administrative, physical, and/ or technical gaps for UNM's CUI information and systems be delivered to Executive Governance, along with a proposed action plan to address those gaps.