Welcome to the CCoE Webinar Series. Our topic today is HIPAA and FISMA: Computing with Regulated Data. Our host is Jeannette Dopheide.

The meeting will begin shortly. Participants are muted. You may type questions into the chat box during the presentation.

This meeting will be recorded.

The CTSC Webinar Series is supported by National Science Foundation grant #1547272.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.
HIPAA and FISMA: Computing with Regulated Data

Susan Ramsey
skramsey@gmail.com
NCAR

and

Anurag Shankar
ashankar@iu.edu
Center for Applied Cybersecurity Research
Indiana University

April 24, 2017
FISMA: Computing with Government Data
What Are We Protecting?

• OPM Breach (2016) cost taxpayers anywhere from $350 million to $1 billion (and still threatens identities)

• Recent attacks on infrastructure include a nuclear power plant, a steel mill, multiple 911 systems, a tornado warning system in Texas; some of these resulted in death

• Integrity of data collected by NOAA ground stations was called into question when an audit found evidence of compromises in 2015 and 2016

References
http://www.nextgov.com/cybersecurity/2016/05/audit-finds-hostile-probes-breaches-commerce-satellite-system/128393/
Compliance is Not Security, But Security Can be Compliance

-- Lance Spitzer, SANS Institute  *Securing the Human: How to Build, Maintain, and Measure a High-Impact Awareness Program*
Federal Cybersecurity Regulations

- Federal Information Security Management Act of 2002
- Defense Federal Acquisition Regulation Supplement (DFARS)(2015 - deadline for compliance 12/2017)

Reference:
https://www.dhs.gov/fisma
http://www.dcaa.mil/dfars.html
When Do Federal Regulations Apply?

• Federal agencies and contractors are subject to FISMA
• NSF as an agency is assessed annually
• NSF awardees have long been expected to apply security best practices aligned to Risk Management Framework
• Agency contracts differ from NSF cooperative agreements
• Contracts may stipulate a FISMA level or
• Specify Controlled Unclassified Information (CUI)
Who Is Responsible?

- Principle Investigators
- Managers and Project Managers
- IT Staff
- HR
- Contracts
- Legal
- Ultimately, the contract holder; the contract can be canceled without an ATO (Authorization to Operate)
NIST Guidelines

NIST - National Institute of Standards and Technology

NIST Risk Management Framework is the FISMA foundation:
• NIST SP 800-37R1 Guide for Applying the RMF
• NIST SP 800-39 Managing Information Security Risk
• NIST SP 800-30R1 Guide for Conducting Risk Assessments

NIST has released 188 “Special Publications” that cover a wide range of functional expectations from cryptography to cloud security
More Than Computer Systems

Includes Organization Policy, People, Process, and Technology

Ex:
• Role-based background checks
  – DFARS, CFRs usually require these as well
• Role based awareness and training
• Processes for evaluating vendor security in contracts
• Physical building access and datacenter safety features
• Media destruction
• Secure coding practices

There are over 1000 NIST operational controls that may be applicable
First - Build a Team

- Executive Sponsor - CIO, CISO, CEO, Board of Directors
- Legal (Privacy Officer)
- Compliance Office (existing HIPAA, PCI or FERPA)
- Contracts
- HR
- Manager of Facilities Security
- Manager of Central/Business IT
- Manager of Identity and Access Management
- IT Security Engineers
- System and Software Administrators/Developers
Timeline and Organization Impact

• If brand new, plan for timeline that includes scheduled meetings and scopes possible organization change
• If you are a PI and don’t have time to project manage this, ask for help from your organization PMO office
  – Or contract a Project Manager
• Identify contacts in Media/Marketing/Communications
• Plan for initial and ongoing education
NIST Risk Management Framework

Risk Management Framework, RMF (SP 800-37)

Step 1: CATEGORIZE Information Systems
- FIPS 199 / SP 800-60

Step 2: SELECT Security Controls
- FIPS 200 / SP 800-53

Step 3: IMPLEMENT Security Controls
- SP 800-160

Step 4: ASSESS Security Controls
- SP 800-53A

Step 5: AUTHORIZE Information Systems
- SP 800-37

Step 6: MONITOR Security Controls
- SP 800-137

Starting Point

Organizational Inputs
- Laws, Directives, Policy, Guidance
- Strategic Goals and Objectives
- Information Security Requirements
- Priorities and Resource Availability

Architecture Description
- Mission/Business Processes
- FEA Reference Models
- Segment and Solution Architectures
- Information System Boundaries

Repeat as necessary

Note: CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).
Step 1: Categorize

- Start with the concept of a “System”
- Identify system boundaries
- Draw and store data flow diagrams
- If planning to use existing IT assets:
  - Create or track down your asset inventory
  - Note how much it will cost you to keep this current!
- If buying new assets, plan your architecture
- Not just hardware any more - include cloud, VMs, software, SAAS, PAAS, Github, Dropbox, O365, Google, OneNote
Map Your Data

• Identify the data stored and transmitted
• Identify Confidentiality, Integrity, Availability (CIA)
• Label data “Low”, “Moderate” or “High” risk to CIA
• Data or services are usually more important than infrastructure (e.g. AWS ELB & Auto Scaling)
• NIST SP 800-60r2 provides guidelines on classification
• Your contract may already specify it for you

Reference:
NIST SP 800-60r2 “Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices
FIPS-199

• Output of this step is called a “FIPS-199” document
  – Create and store your FIPS-199 with revision control

Things you start thinking about during this step:
  – Data and Services are usually what we’re protecting
  – Confidentiality, Integrity, Availability - what’s important to me?
  – “Locking up a box” vs protecting CIA for data and services

Reference:
FIPS Pub 199 “Standards for Security Categorization of Federal Information and Information Systems”
Step 2: Select

• You identified a Low, Moderate, or High risk “baseline” in your FIPS-199
• Use NIST SP 800-53r4 to select controls that match your baseline
• If CUI, use NIST SP 800-171 as your baseline
• To reduce cost and complexity, try to tailor out any controls that your system does not need

Reference:
NIST SP 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
# Example Control

## AC-2

### ACCOUNT MANAGEMENT

**Family:** AC - ACCESS CONTROL  
**Class:**  
**Priority:** P1 - Implement P1 security controls first.  
**Baseline Allocation:**

<table>
<thead>
<tr>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-2</td>
<td>AC-2 (1) (2) (3) (4)</td>
<td>AC-2 (1) (2) (3) (4) (5) (11) (12) (13)</td>
</tr>
</tbody>
</table>

## Control Description

The organization:

- Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
- Assigns account managers for information system accounts;
- Establishes conditions for group and role membership;
- Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
- Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
- Monitors the use of information system accounts;
- Notifies account managers:
  1. When accounts are no longer required;
  2. When users are terminated or transferred; and
  3. When individual information system usage or need-to-know changes;
- Authorizes access to the information system based on:
  1. A valid access authorization;
  2. Intended system usage; and
  3. Other attributes as required by the organization or associated missions/business functions;
- Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and
- Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
FIPS-200

• Output of this step is called a “FIPS-200” document
  – Create and store your FIPS-200 with revision control
• This is a description of the System and a list of controls that will be assessed
• Document any tailoring in the FIPS-200
• Copy and paste all your selected controls into a System Security Plan (SSP) for the next step

Reference:
Step 3: Implement

Your System Security Plan (SSP) is a “living” record of:

• Policies
• Standards
• Procedures
• Roles
• Overlays
• Implementation Details

Reference:
Implement Examples

- Example Policy:
  AC-1 “The organization has a policy on Access Control.”

- Example Standard:
  “All Access Control follows the principle of least privilege.”

- Example Procedure:
  “Authorized Domain Administrators limit access control to least privilege through applying GPO settings in the Windows MMC plugin.”

Reference:
NIST SP 800-53a Assessing Security and Privacy Controls in Federal Information Systems and Organizations
Roles and Responsibilities

- It is fundamental to define Roles and Responsibilities
- Ownership and Accountability are tenants of FISMA

Make sure you define and record who does what, when, in your SSP. “Ex: The PI is responsible for updating the SSP annually”.
  - Create and store your SSP with revision control
  - Plan to update it annually or more often

Reference:
NIST SP 800-53 Security Controls and Assessment Procedures for Federal Information Systems and Organizations
More Plans

You may also have contractual requirements to submit formal plans to describe how you manage:

- Business Continuity (including Disaster Recovery)
- Business Impact Analysis
- Risk Assessment Report/Plan
- System Configuration
- Continuous Monitoring
- Inter-System Agreements
- Incident Response

Reference: http://csrc.nist.gov/publications/PubsSPs.html#SP 800
Step 4: Assess

- Internal or External determined by your classification
- FISMA Moderate requires Independent Assessment (unless you successfully tailored it out)
- NIST SP 800-171 does not
- Familiarize yourself with NIST SP 800-53a, Assessing Security and Privacy Controls in Federal Information Systems and Organizations
- Practice with your team, and have all your paperwork ready
Be Active in Your Assessment

You will want to manage your Independent Assessment process:
• Choose a respected company that has proven FISMA experience
• Many professional auditors are more familiar with PCI
• Check with your AO if they have a preference
• Agree to your Security Assessment Plan (SAP)
• Negotiate findings in your Security Assessment Report (SAR)
Plan of Action and Milestones

• The output of the Assessment is a Security Assessment Report (SAR)
• You own your SAR
• You send your SAR to your AO (or can share internally)
  – Store your SAR with revision control
• Findings become addressed in POA&Ms
• POA&Ms are ongoing
Create a POA&M Repository

It’s at this point you realize that RMF is a cleverly disguised version of Continuous Process Improvement

• Create a repo and a process for POA&Ms
  – Formal documents that acknowledge gaps, and promise measurable remediation
  – Turn them into SMART goals

• Progress is communicated to your AO on established schedule

• Coordination on POA&Ms crosses teams (HR, Contracts, etc)
Step 5: Authorize

- Sites that are adopting RMF and NIST SP 800-53 or NIST 800-171 control guidelines for internal purposes do not need to obtain external authorization.
- However, even in an internal RMF, someone is expected to be an AO and sign their name to an Authorization to Operate.
- The AO ultimately accepts and owns the risk.
Authorization or Authority

• The output of this step is your ATO
  – Store your ATO with revision control and update it if any of the
    real people named in it leave their positions
• It may be more or less formal for your organization
• There are no criminal penalties for violating FISMA but ATOs
  can be revoked, or can be allowed to expire
• Might face breach of contract

Reference:
http://www.csoonline.com/article/3112677/leadership-management/nasa-cio-allows-hpe-contract-to-expire-refuses-to-sign-off-
on-authority-to-operate.html
Step 6: Monitor

Three tiers of Continuous Monitoring:
• Organization Policy
• Business Processes
• POA&Ms
• Information Systems controls, status, metrics collection
• Not just “network monitoring”
• Create a plan or bake it into ops

Reference: NIST SP 800-137 Information Security Continuous Monitoring
Who Does What, When?

Tier 1: Policy Review - Who does it and how often?
Tier 2: Procedure Review - Who does it and how often?
Tier 3: These can be expensive
   • Vulnerability Scan, Assessment and Remediation
   • Configuration and Patch Remediation
   • Vendor, Service and Product Risk Assessments
   • Audit Log Aggregation and Alerting (SIEM)
   • Intrusion Detection/Prevention and Response
   • Incident Response
   • Metrics Collection and Reporting
   • Awareness and Training Attendance
Determine and Collect Metrics

Collect **metrics** that will be most useful:

- % Windows 10 endpoints patched in 48 hours
- % patched vs unpatched Win10 endpoints that get compromised
- Percentage of CentOS 7 servers under Puppet control
- Amount of downtime in hours per month due to unauthorized configuration changes
- Number of SQL Slammer attacks blocked at firewall per month
- Number of successful password brute force attempts per month
- Number of successful phished passwords per month
- Amount of downtime in hours per month due to DDOS
- Dollar cost of reconfiguring systems due to successful ransomware

Reference: NIST SP 800-55r1 *Performance Measurement Guide for Information Security*
Beyond Continuous Monitoring

- OMB, DHS, NSA, DOD, Army, Navy ... found that Systems were FISMA compliant but not secure.
- Why? People were “monitoring” but not fixing
- In 2014, DHS started managing FISMA (originally DOC)
- DHS emphasis now is on Continuous Diagnostics and Remediation, NIST Cybersecurity Framework
- Changes to Reporting Requirements
- Information sharing - breach detection, forensics
- 48 hour incident notification

Reference: https://www.dhs.gov/cdm
The CF is more outcome-oriented (Rather than descriptive)

- Identify
- Protect
- Detect
- Respond
- Recover

New draft published this year, comments period ended April 10, 2017.

Reference: https://www.nist.gov/cyberframework
RMF vs Cybersecurity Framework

RMF: Decide *why* (risk) and *how* (controls) you are going to make it safe

- *Ex:* *It took an average 20 minutes to compromise an unpatched Windows XP system* *(SANS, 2004)*

Cybersecurity Framework: Score yourself on (and improve) the actions that you are taking to keep it safe

- *Ex:* *M-trends reports that APT/infections exist for 200 days, on average, before they are detected* *(Mandiant/FireEye, 2016)*
Management Framework

Complex but not rocket science to those familiar with:
- ITIL
- COBIT
- PMI
- EFQM

This, however, is a huge deviation from rocket science!!

Best chances for ongoing success
- Establish team/program
- Leverage organizational resources
Health Insurance Portability and Accountability Act (HIPAA)

- Comprised of the HIPAA Privacy Rule, Security Rule*, and breach notification.
- The Privacy Rule defines who HIPAA applies to (covered entities), what is protected (protected health information or PHI), and covers disclosures.
- The Security Rule focuses exclusively on how to protect electronic PHI (ePHI*) in any form – at rest, in transit, in memory, etc.

* ePHI = identifiable patient data with one or more of 18 identifiers

* Of most concern to IT providers
HIPAA Security Rule*

The Security Rule requires 1. Administrative, 2. Physical, and 3. Technical safeguards to

- Ensure the confidentiality, integrity, and availability of ePHI created, received, maintained or transmitted;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures;
- Ensure compliance by the workforce; and
- Provide a means for managing risk in an ongoing fashion.

* Enforced by the Office for Civil Right (OCR) within the US Dept. of Health and Human Services (HHS)
Who is covered by HIPAA?

Only two types of organizations:

1. a **covered entity (CE)** = a healthcare provider, health plan, or health clearinghouse

2. a **business associate (BA)** = an external entity that serves a CE and creates, receives, maintains, or transmits PHI for them

If you are BA, you must have a HIPAA Business Associate Agreement (BAA) with the CE
NSF and HIPAA

- NSF funds human subjects research (e.g. in psychology), which is subject to the Common Rule*.

- HIPAA comes into play when a NSF funded project engages in activities involving identifiable health data, e.g. testing engineering sensors for diabetes control.

- Health data is also rapidly leaking into NSF facilities such as HPC centers.

Is health data a target?

• Yes, very much. Healthcare was the second most heavily targeted sector in terms of breaches in 2016.

• Why? Because a health record is a conveniently pre-packaged, easily exploitable bundle of data including personal, health insurance, and credit card info.

• Cybercriminals use it for identity & insurance fraud, blackmail/extortion, snooping, etc.
Black Market Rates*

- Medical records: $82.90
- Physical location info: $38.40
- Marital status: $6.10
- Name and gender: $2.90
- Social Security Numbers: $55.70
- Payment details: $45.10

* Privacy Rights Clearinghouse data survey
HIPAA Challenges

• HIPAA is fuzzy = not prescriptive*; you have to interpret it yourself.

• => it’s confusing without in-house compliance expertise. Commercial consultants can help, but can be beyond reach due to cost.

• Peers are not always easy to find.

=> misinterpretation/fear; drastic, unneeded reaction.

* It tells you to maintain “reasonable and appropriate” safeguards
Is all health data ePHI?

• No. Only data created, received, maintained, and transmitted by CEs (or by BAs for CEs) is bound by HIPAA. Identifiable health data outside a healthcare context is not.
• ePHI, when properly de-identified, becomes non-ePHI.
• There are a few other contexts where identifiable health data is not subject to HIPAA.
How do I tell if I’m compliant?

- You don’t. HIPAA compliance is not deterministic. You can only do due diligence. (The OCR may still find you lacking.)
- No one is authorized by HHS to certify HIPAA compliance.
- HIPAA-required risk management, once started, becomes an ongoing, baseline activity as long as there is ePHI on the system.
HIPAA @ Indiana University

- Scope: IU’s large central IT, including its research cyberinfrastructure.
- IU was an early implementer of HIPAA for its research computing. We developed a HIPAA specific process* in 2008 to support clinical research at the IU School of Medicine.
- By 2013, other rules & regulations such as FISMA loomed, requiring a new, more unified vision for cybersecurity and compliance.

* Overseen by a committee of primary stakeholders
Risk Management Framework

A RMF addresses risk holistically. It covers:

- Governance = institutional security organization, policies, sanctions, enforcement
- Risk management = assessment, mitigation through appropriate physical, administrative, technical controls, documentation
- Review = regular monitoring, reviews, reassessment, and mitigation
- Awareness and training

One of the most comprehensive is the NIST Risk Management Framework (RMF)
Choosing the RMF @ IU

You can choose FAIR, OCTAVE, ISO, etc., but NIST was a natural choice for us because:

• It is a cybersecurity standard
• It can be tailored easily
• It can address both HIPAA & FISMA (+ other, federal and state rules and regulations)
• It is ideal for government funded institutions
The Current IU Approach

Manage risk first, compliance will follow

1. Establish a NIST-based risk management framework.
2. Use HIPAA to NIST mapping (already done by the government in NIST 800-66) for compliance.
3. Explicitly address remaining HIPAA safeguards that do not map to NIST.
   Focus on minimizing total risk rather than creating walled gardens
Establishing an RMF

1. Inventory and document existing policies/procedures and common controls.
2. Develop a risk management process for individual systems.
3. New systems simply “join” the existing RMF, expanding it for subsequent systems/projects.
The IU NIST Process

1. Inventory
2. Risk Assessment
3. Risk Response
4. Training
5. Oversight
6. Ongoing Risk Management
1. System Inventory

- System details, ePHI location, major security settings, BAAs, vuln. scan dates, access mechanisms, disposal information, etc.
- Software version, patch level, BAAs, etc.
- Privileged access - names, roles, dates authorized, etc.
- Incident log – incident summary, response.
Current Controls Inventory

- Our NIST-based process also inventories controls.
- Documented in a System Security Plan or SSP.
- It includes system details, categorization, roles and responsibilities, contacts, purpose, components, interconnections, data flows, boundaries, dependencies.
- ... and the NIST 800-53 security & privacy controls currently in place.
What is NIST 800-53?

- A catalog of ~1000 security and privacy controls*
  - Divided into control families such as “Access Control (AC)”, “Awareness & Training (AT)”, etc.
- Defines security baselines – LOW, MODERATE, and HIGH, with increasingly more controls.
- Using a large catalog adds completeness and rigor and prevents you from overlooking controls you might otherwise.

* 800-171 is ~100 controls
These map to HIPAA safeguards

* We can give you a ready-to-use, complete doc template package
2. Risk Assessment

- We do an internal risk self-assessment.
- Managers & sys admins brainstorm together to identify areas of vulnerabilities and risk. Many are already apparent from documenting existing controls.
- The Risk Assessment Report documents risk areas, existing controls that address those risks, residual vulnerabilities and risks, and risk severity.
Risks

- System risk – lack, misapplication, or failure of physical/technical controls at the system end.
- User risk – unsafe workflow or system use at the user end.
- Governance risk – lack, misapplication, or failure of administrative controls.

Total Risk = Sum of all three
Workflow Risk

• We include the user workflow also for end to end HIPAA security. Just the system isn’t enough. HIPAA affects the entire CE/BA, not a system or a user.
• Representative research use cases/workflows are identified and ”risk-optimized”.
• This also helps and guides the users to do the right thing. You cannot ask them for security without giving them tools.
### Research use case/workflows

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 A research team wants to store and share working data that can be accessed on user desktops as a &quot;drive&quot; via the web, and from an II VM</td>
<td>Use RFS. Install an OpenAFS client on Windows/Linux desktops and the II VM and set up RFS ACLs to authorize access for team members.</td>
</tr>
<tr>
<td>2 A research team wants to archive massive amounts of data for 6 years and share the archive</td>
<td>Use SDA. Pack the data in large chunks before storing. Set up SDA ACLs to authorize access for team members. Use the SDA web interface or CIFS/Samba to map a drive.</td>
</tr>
<tr>
<td>3 A researcher wants to manage data remotely via the web but wishes to avoid using a browser on the local desktop workstation for enhanced security</td>
<td>Log into IUnaryWare and use a browser there. This not only avoids using a local browser (except to access IUnaryWare), it enhances security further owing to the fact that all operations in IUnaryWare occur in reality on a Citrix server. The browser a user sees is merely a virtual representation of the browser process running on the server.</td>
</tr>
<tr>
<td>4 A research team wants to publish massive amounts of data via the web</td>
<td>Develop a web application that uses the HPSS API to access the SDA. The consumer may incur a time penalty (up to a minute) before the data is read from tape.</td>
</tr>
<tr>
<td>5 A research team wants to examine and manage data which is stored in Excel or CSV files and export managed data for Ingest by statistical packages such as SAS, SPSS, etc.</td>
<td>Import data into REDCap. Log into REDCap, set up ACLs to authorize access for team members, and manage/export data. REDCap allows one to develop surveys using point and click, manage tabular data, share it with IU/Non-IU users, and export in a comma delimited format readable by SAS, SPSS, R, Excel, etc.</td>
</tr>
<tr>
<td>6 A research team wants to analyze data using a Windows stats package</td>
<td>Use the pre-installed statistical packages in IUnaryWare. Transfer data into Box Health Data Account, log into IUnaryWare, import data from Box, launch the application to analyze data, and</td>
</tr>
</tbody>
</table>
3. Risk Response

- A Plan of Action & Milestones documents the response to each residual risk.
- Response = whether the risk was accepted, transferred, addressed, or to be mitigated, and reasons, timelines and planned mitigation activities/controls.
- Valid reasons for accepting a risk may be budget, resource constraints, etc. We try our best to address them, often through policies/procedures & training.
4. Staff Training

- Annual training is mandatory for both management and staff responsible for the system.
- Three e-training modules must be completed:
  1. IU HIPAA training (covering the law and IU policies & procedures)
  2. IU Human Subjects training
  3. Central IT specific information on how HIPAA applies to our systems, the NIST RMF, and local policies & procedures
- All compliance and security training is documented.
User Training

• We provide online training and awareness via our Knowledge Base, YouTube videos, local media, in person classes, security site, and email alerts.
• We make users understand that IU is HIPAA compliant only when they do their part, not just because the system has HIPAA safeguards.
• We train them and help them document safeguards at their end.
5. Oversight

- The completed compliance package is sent to the University HIPAA Privacy and Security Officers, Information Security Office, and Internal Audit for review.

- HIPAA compliance is self-asserted at IU today, but this is changing.
6. Ongoing Risk Management

- Once a system becomes part of the RMF, it becomes subject to regular, ongoing risk management until decommissioning.
- We do:
  - Semi-annual reviews, risk re-assessments, and documentation updates
  - Continuous, automated monitoring of systems
  - Annual training
  - Oversight
  - External assessments
Resilience

- Resilience - a new movement within cybersecurity.
- Accepts reality - that attacks/breaches are like germs/diseases, inevitable and ubiquitous.
- … so why not use the same approach that medicine uses to treat disease?
- = focus on prevention, detection, response, and recovery, assuming constant attacks.

Prevention = risk management, Detection = real-time telemetry and alerts, Response = manual/automated reactions to alerts, incident response, Recovery = DR, BCP
Outcomes

- NIST RMF has allowed us to establish a unified approach to cybersecurity and compliance.
- It has prepared us for FISMA contracts.
- Units engaged in compliance like the process.
- Everyone sends customers/$$ our way.
- We are confident in our ability to handle audits.
Many safeguards are typically already in place.
You just need a risk management structure and documentation, a one-time heavy lift exercise (ongoing is a lot easier).
Managing cyber risk holistically leads to compliance as a byproduct.

The government does not expect you to undertake herculean measures/build walled gardens
Thank You!

Questions?

Please take our survey.
About the CTSC Webinar Series

To *view* presentations, *join* the discuss mailing list, or *submit* requests to present, visit:

http://trustedci.org/webinars

*The next webinar is May 22nd at 11am Eastern*

*Topic: Cybersecurity Research: Transition to Practice*

*Speakers: Emily Nichols and Alec Yasinsac*

The CTSC Webinar Series is supported by National Science Foundation grant #1547272.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.
Thank You

We thank the National Science Foundation (grant 1547272) for supporting our work.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.