

Data Management & Security Panel

University of Arizona
College of Medicine



Andrew Mahler

- Background:
 - Lawyer, Federal Investigator, HHS (Office for Civil Rights)
 - CIPP/US, CHRC, CHPC
 - Experienced in health and human subjects research rules and regulations
- Current:
 - HIPAA Privacy Officer (UA – reporting to Sr. Director, Human & Clinical Research Services)
 - Research Integrity Officer (UA – reporting to Sr. Vice President for Research)

HIPAA Privacy Program

- Privacy Officer required by the U.S. Department of Health & Human Services (*HHS*), Office for Civil Rights (*OCR*)
- HIPAA applies in the healthcare context and related activities
 - Providers, health insurers
 - Business associates
 - Research
 - Public health
- Main goal:
 - Patient privacy and security

HIPAA & The University of Arizona

HIPAA Healthcare Components

- Covered entity and business associates
- Must comply with Privacy, Security, and Breach Notification Rules

Human subjects research

- Must comply with HIPAA to the extent the Rules apply to human subjects research

About the HIPAA Privacy Program

The HIPAA Privacy Officer oversees the following activities:

- Identification of departments, clinics and offices that have HIPAA obligations
- Development and implementation of policies and procedures
- Review of all Business Associate and Data Use Agreements
- Security Rule risk analysis (in partnership with the Information Security Office)
- Training and outreach
- Breach notification and mitigation
- Assistance to University researchers who require PHI.



Privacy & Security



U.S. Privacy & Data Protection Regime

- The U.S. Constitution does not explicitly provide a right to privacy.
- The Sectoral Model (U.S.)
 - Limited federal involvement in privacy or data management
 - Usually self-regulation for sectors that are not subject to specific statutes
 - Creates different legal requirements for healthcare and financial services (2016)



5 Questions to Consider...

1. Does your data require compliance with federal or state law?
 2. Does your data require compliance with a contract or other agreement?
 3. What safeguards are in-place for physical data? For electronic data?
 4. What protections did you specify in your application?
 5. Does your project require identifiable data (human subjects)? If not, de-identify!
- 

Data Classification Tiers

University of Arizona

INTERNAL	PUBLIC	CONFIDENTIAL	REGULATED
Data not intended for public use or exposure. Internal data generally should not be disclosed outside of the University without the permission of the person or group that created the data. Any data not specifically classified as Regulated, Confidential, or Public should be considered Internal.	Data that may be disclosed to any person, regardless of affiliation with the University. Some level of control is required to protect the integrity and availability of Public data (e.g., protecting original (source) documents from unauthorized modification).	Data protected as Confidential by law, contracts, or third-party agreement, and by the University for confidential treatment. Unauthorized disclosure, alteration, or destruction of this data type could cause a significant level of risk to the University or its affiliates.	Data controlled by federal, state, local, and/or industry regulations. These data are affected by data breach notification laws and contractual provisions in government research grants, which impose legal and technical restrictions on the appropriate use of institutional information.

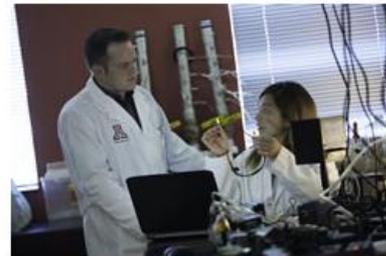
The Research Gateway

rgw.arizona.edu

[Directory](#) [Feedback](#) [Site Index](#)



Research
Research Gateway



Information Security security.arizona.edu

THE UNIVERSITY OF ARIZONA®



Information Security

About Us >

Report an Incident >

Governance >

Policy and Guidance >

SecureCat Courier >

Security Tips/Resources >

Faculty and Staff >

Students >

Security for IT Professionals >

Privileged Data Users >

UA NetID+ >

UA VPN Client >

Spotlight >

Upcoming Events >

Policy and Guidance

UA Information Security (UAIS) is responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University. UAIS is also responsible for coordinating various regulatory compliance efforts as they relate to information technology systems.



[POLICIES](#)

[STANDARDS](#)

[GUIDELINES](#)

Cybersecurity Framework

The [University of Arizona's Cybersecurity Framework](#) is based on [NIST's Framework for Improving Critical Infrastructure Cybersecurity](#). The Framework is a risk-based approach to managing cybersecurity risk.

Additional tools and guidance to help units conduct self-assessments will be coming soon.

Policies: High level statements, equivalent to organizational law, that drive decision making within the University. University policies are subject to a rigorous review process. The University's information security policies reside on the University's [policy](#) website.

- [Information Security Policy \(IS-100\)](#)
- [Computer and Network Access Agreement \(IS-700\)](#)



[POLICIES](#)

[STANDARDS](#)

[GUIDELINES](#)



THE UNIVERSITY
OF ARIZONA

Cybersecurity Considerations for Healthcare Researchers

Christian Schreiber, CISM, PMP
University Information Security Officer

Presented 22 March 2016

Personal Background

- CISO & HIPAA Security Officer at the University of Arizona since 2012
- 8+ years leading information security programs at universities and Fortune 500 organizations
- Nearly 20 years IT & information security leadership experience
- Joining leading cybersecurity company FireEye as a consultant specializing in higher education and government risk
- Education & Professional Certifications
 - Masters Certificate in Project Management, University of Wisconsin – Madison
 - Bachelor of Science in Business Administration, Central Michigan University
 - Certified Information Security Manager (CISM)
 - Project Management Professional (PMP)
 - IT Service Management Foundations (ITIL)





THE UNIVERSITY
OF ARIZONA

What is information security?

And why does it matter beyond being “an IT problem”?

UA Information Security mission

To support the University of Arizona's research and education mission by enabling the University community to mitigate risk to information assets.

What are “Information Assets”?

Any data, system, computer, network device, document, or any other infrastructure component that stores, processes, or transmits University data

- More than just “the computers”
- Regulations require protection of written documents
- Some regulations (e.g. HIPAA) include protection of verbal as well as written and electronic communication

Information assets can be hard to define and locate!

Think about a typical university for a minute...

Different Sources

Students

Parents

Alumni

Sports Fans

Visitors

Applicants

Employees

Conference Attendees

Study Participants

Received in different ways

Mailed In

Telephone

In Person

Internet

3rd Parties / Partners

Stored in different places

Paper records

Servers

Desktops

Laptops

“The Cloud”

Network drives

Spreadsheets

Email

Portable drives

Smartphones

What kinds of data do cyber criminals go after?

Commonly targeted types of information assets*

Sensitive Enterprise Data

- Employee data
- Student records
- Financial data
- Recruitment and marketing data

Research with Potential Economic Value

- Energy technology
- Biotechnology, medical, and pharmaceuticals
- Engineering
- New materials, such as semi-conductors
- Information technology

Politically or Commercially Sensitive Information

- Climate modelling
- Economic data and projections
- Live animal research
- Product development data
- Information used for expert testimony

Why would a cyber criminal target MY organization?

Organized Crime

- Financial gain

Hacktivism

- Disruption for political reasons

Economic Espionage

- Theft of intellectual property

Pass-through Attacks

- Exploit resources for further attacks

Destructive Attacks

- Disrupt operations and destroy data

Just how bad can it be?

FireEye report: Maginot Revisited

Studied more than 1,600 organizations in 2014

- 96% breached
- 27% involved advanced attacks

Education industry worse!

- 100% breached
- 37% involved advanced attacks



Why so bad? Cybersecurity is asymmetric

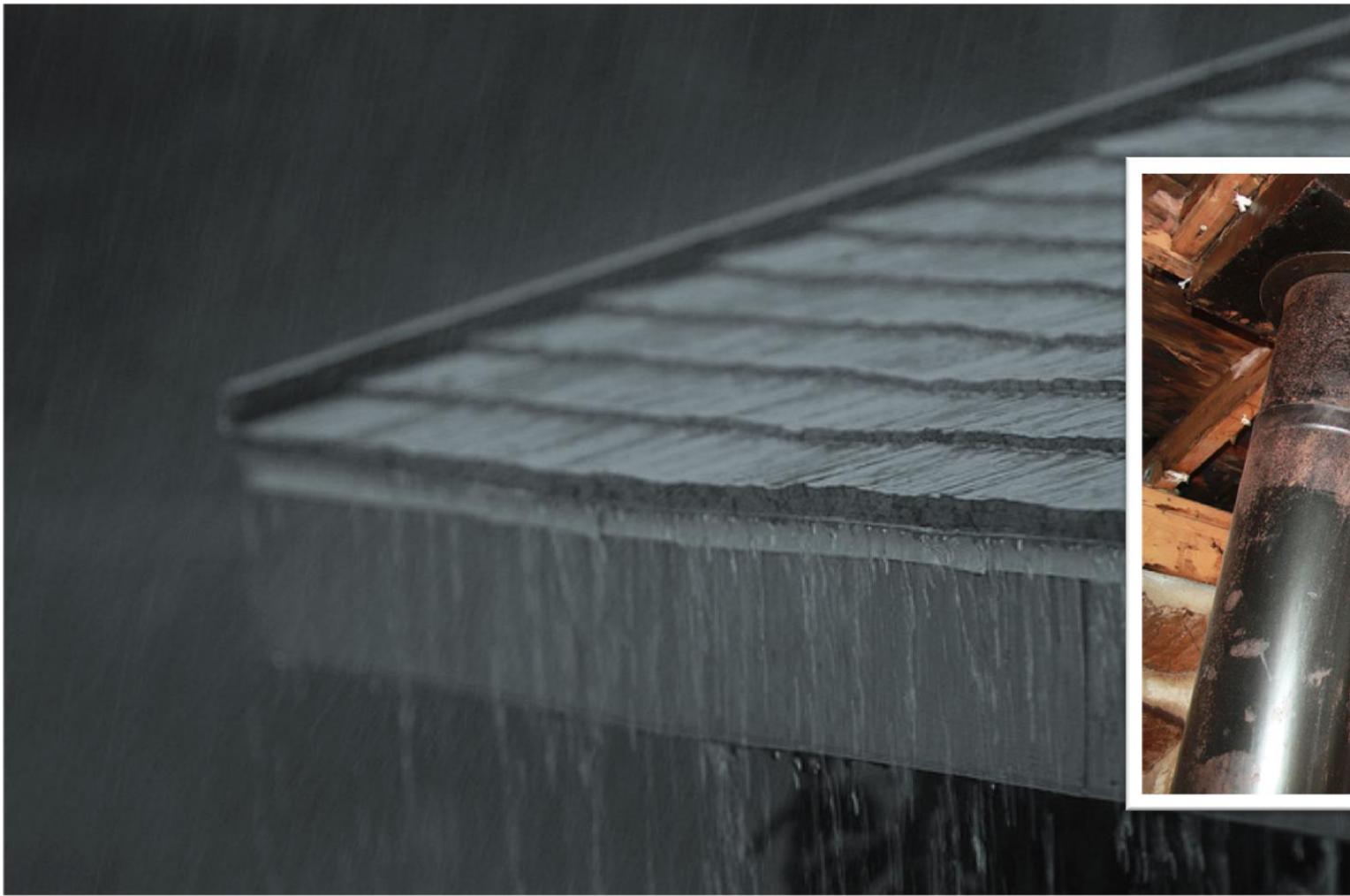
Defenders need to succeed 100% of the time and invest heavily to design robust solutions

Attackers only need one win!

- One successful phishing email and attackers can be inside, regardless of the amount invested in perimeter defenses!



How should we think about our security metrics?





THE UNIVERSITY
OF ARIZONA

Remember that YOU are a target!

Protect your user credentials, computers,
and mobile devices from attackers

Attackers use compromised credentials to carry out more than 95% of data breaches*

Attackers use phishing emails and malware to gain access to usernames and passwords

Once they have credentials, attackers simply log into the systems they are targeting



Use Global NetID+ to protect your account

Multifactor authentication prevents attackers from impersonating you, even if they get your password!

- Make sure to register for the “Global” option so that your NetID always prompts for the token
- Use the “remember device” feature so computers you use frequently only prompt once per month



Keep your devices patched and run antivirus

71% of computer compromises used vulnerabilities more than a year old*

Remember to patch and run antivirus on all your devices!

- Enable automatic updates when possible
- University site license for Sophos runs on Windows and Apple devices
- Sophos antivirus also available in app stores for iOS and Android mobile devices



Encrypt your devices

Reduces likelihood of unauthorized access to data on the device

- Important when investigating / documenting lost devices that stored sensitive data

Encrypt your laptops, external storage devices, and mobile devices

- May need to encrypt servers and desktops depending on compliance requirements





THE UNIVERSITY
OF ARIZONA

Protecting research data

Compliance and data protection requirements vary. Make sure you track changes from your sponsors and contracting authorities!

Regulatory requirements on the horizon

Changes are gaining momentum in federal agencies. Make sure you're prepared!

Executive Order 13556 "Controlled Unclassified Information"

- Issued November 2010
- Replaces May 2008 Presidential memorandum

In the past few months, UA has received several research contracts that include cybersecurity compliance clauses



Controlled Unclassified Information Program

Established by Executive Order 13556 – November 2010

Manages all unclassified information within the executive branch that requires safeguarding and dissemination controls as required by law, regulation, and Government-wide policy.

- National Archives and Records Administration (NARA) designated as Executive Agent to implement the Order and oversee agency actions to ensure compliance

22 Categories		85 Subcategories
1. Agriculture	12. Law Enforcement	• Bank Secrecy • DNA • Investigation
2. Copyright	13. Legal	
3. Critical Infrastructure	14. NATO	
4. Emergency Management	15. Nuclear	• Financial • Health Information • Personnel
5. Export Control	16. Patent	
6. Financial	17. Privacy	
7. Foreign Government	18. Proprietary	• Census • Investment Survey
8. Geodetic Product Information	19. Safety Act Information	
9. Immigration	20. Statistical	
10. Information Systems Vulnerability Information	21. Tax	
11. Intelligence	22. Transportation	

Why are cybersecurity requirements added to contracts for research that doesn't appear overly sensitive?

CONFIDENTIALITY most commonly discussed security requirement

- Stealing sensitive personal information, credit cards, etc. for financial gain

AVAILABILITY and **INTEGRITY** are often overlooked risks

- Destroying years of research data making it unrecoverable
- Modifying research data to produce inaccurate results



Updates to federal cybersecurity guidance in 2015

National Archives and Record Administration (NARA)

- Proposed CUI Federal Regulation 32 CFR 2002 (May 2015)

National Institute of Standards and Technology (NIST)

- SP 800-171 “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (June 2015)

Office of Management and Budget (OMB)

- “Improving Cybersecurity Protections in Federal Acquisitions” (August 2015)

Defense Federal Acquisition Regulation Supplement (DFARS)

- “Network Penetration Reporting and Contracting for Cloud Services” (August 2015)



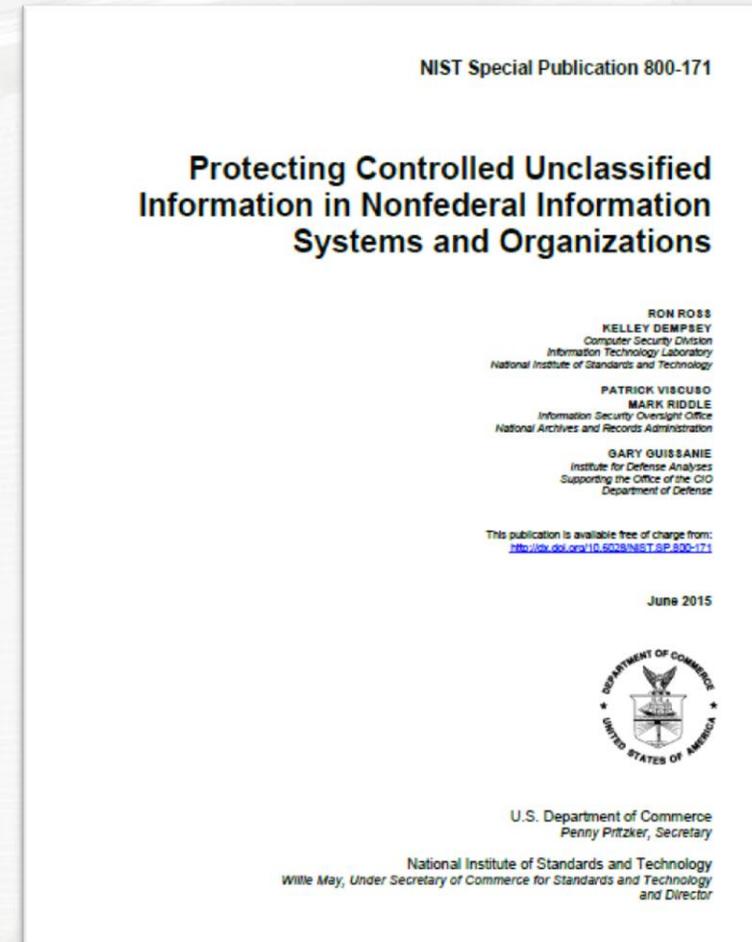
Federal government contractors handling Controlled Unclassified Information (CUI) should take notice of [the] recent executive agency actions. Combined, they lay the groundwork for a new cybersecurity clause to be added to the Federal Acquisition Regulation (FAR) in 2016.

- Mary E. Bosco, Holland & Knight LLP. 17 July 2015. Available online at <http://www.jdsupra.com/legalnews/actions-foreshadow-uniform-45314/>

How do these changes impact research contracts?

2015 OMB and DFARS guidance establish similar cybersecurity requirements

- Implement NIST 800-171 or equivalent security controls
- Investigate and promptly report cybersecurity incidents to federal authorities (72 hour time limit)
- Conduct security assessments and document / submit the results
- Implement “Information Security Continuous Monitoring”



Requirements are becoming more concrete with compliance deadlines and more defined process expectations

For example, Department of Defense has set expectations for contractors that may interact with “Controlled Defense Information”

- Contractors must implement 800-171 standards “as soon as practical, **but not later than December 31, 2017.**”
- Contractors must notify the DoD Chief Information Officer (CIO) within 30 days of award about any 800-171 security requirement that has not been implemented at the time of contract award.
- An “authorized representative of the DoD CIO” will “adjudicate” requests for variances from the 800-171 requirements prior to contract award, and any accepted variance “shall be incorporated into the resulting contract.”
- The exact phrasing of the clause must be flowed down to subcontractors “without alteration,” except as needed to identify the contracting parties subject to the clause.



Are these changes really filtering down to universities?

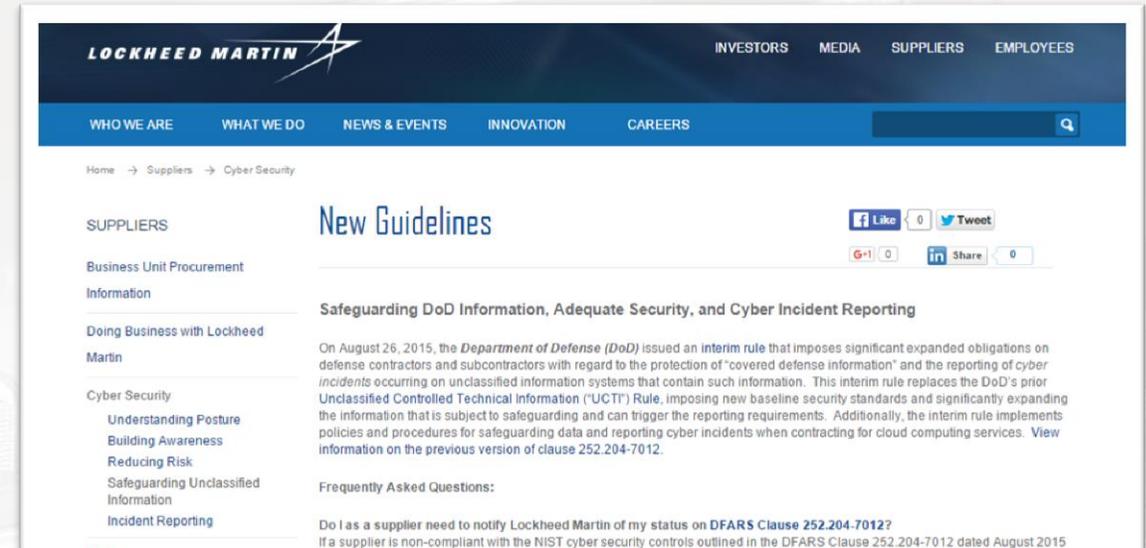
Department of Homeland Security Acquisition Regulation

Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement Clause 252.204-7012 (Safeguarding Unclassified Controlled Technical Information)

Version 2.0

August 2015

Office of the Deputy Assistant Secretary of Defense for Systems Engineering
Washington, D.C.



The screenshot shows the Lockheed Martin website's 'Suppliers' page. The header includes the Lockheed Martin logo and navigation links for Investors, Media, Suppliers, and Employees. Below the header, there are tabs for 'Who We Are', 'What We Do', 'News & Events', 'Innovation', and 'Careers'. The main content area is titled 'New Guidelines' and includes social media sharing options for Facebook, Twitter, and LinkedIn. The text on the page discusses 'Safeguarding DoD Information, Adequate Security, and Cyber Incident Reporting' and mentions an interim rule issued by the Department of Defense on August 26, 2015, regarding the protection of 'covered defense information' and the reporting of cyber incidents. It also includes a 'Frequently Asked Questions' section with a question about whether suppliers need to notify Lockheed Martin of their status on DFARS Clause 252.204-7012.

If a supplier is non-compliant with the NIST cyber security controls outlined in the DFARS Clause 252.204-7012 dated August 2015 or later, then the supplier must notify Lockheed Martin through the authorized procurement representative identified in the subcontract or purchase order.

- Lockheed Martin. "New Guidelines." Available online at <http://www.lockheedmartin.com/us/suppliers/cyber-security/dfars.html>

Remember to factor in cybersecurity requirements while planning projects and proposals

UA has developed cybersecurity compliance plans for small projects

- Information Security, ORD, and researchers developed technology control plans for small projects with isolated computers
- **These plans prohibit researchers from connecting computers that process, transmit, or store CUI to any non-isolated network or to the Internet**

Additional investment will be needed for larger projects and network-connected computing environments





THE UNIVERSITY
OF ARIZONA

Questions?

Christian Schreiber, CISM, PMP
schreiber@email.arizona.edu

<http://security.arizona.edu>
<https://www.linkedin.com/in/christianschreiber>