National Institute of Allergy and Infectious Diseases

Drupal GovCon 2015

Drupal + FISMA

Lessons Learned Using Drupal within the Federal Information Security Framework

Nick Weber, MS, PMP
NIAID Scientific Computing Project Manager

Metasebia Gizaw, CISSP, CEH
NIAID Security Engineer (Contractor)

23 July 2015

NIAID

National Institute of Allergy and Infectious Diseases

Obligatory Disclaimer

(Sorry – we're in the government!)

National Institute of Allergy and Infectious Diseases

NIAID

Security Breaches

Recent incidents impact us and shape our perspectives

- **WHEN**: December 2013
- **WHAT**: Names, mailing addresses, email addresses, phone numbers, credit/debit card information compromised
- **HOW**: Via third party vendor that had authorized access to Target network
- **WHO**: 70 million customers affected by the breach
- **HOW MUCH**: >$200M in recovery and associated costs

NIH National Institute of Allergy and Infectious Diseases

NIAID

Security Breaches

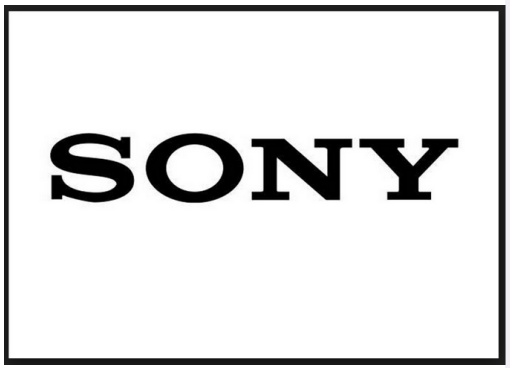
Recent incidents impact us and shape our perspectives

- **WHEN**: November 2014
- **WHAT**: Credit card numbers, email addresses
- **HOW**: Via stolen third party username and password
- **WHO**: 56 million credit cards numbers, 53 million email addresses
- **HOW MUCH**: $62M in recovery and associated costs

Sources: 2, 3

Security Breaches

Recent incidents impact us and shape our perspectives



- **WHEN**: November 2014
- **WHAT**: Large-scale, targeted attack of the Sony datacenter; contracts, salary lists, film budgets, entire films, emails, and names/Social Security numbers
- **HOW**: Targeted attack by “Guardians of Peace” group, purported to be from North Korea
- **WHO**: Current and former employees, executives
- **HOW MUCH**: Caused embarrassment to company and management team as well as loss of revenue

Security Breaches

Recent incidents impact us and shape our perspectives

- **WHEN**: February 2015
- **WHAT**: Social Security numbers, birth dates, addresses, emails, employment information, income data
- **HOW**: Targeted attacks to steal network credentials of a few employees with high-level system access
- **WHO**: 80 million current and former customers, as well as employees

Security Breaches

Recent incidents impact us and shape our perspectives

- **WHEN**: June 2015
- **WHAT**: SSN; residency and educational history; employment history; information about immediate family and other personal and business acquaintances; health, criminal, and financial history; findings from interviews conducted by background investigators; fingerprints, usernames and passwords for background investigation form
- **WHO**: 4.2 million current and former employees; 19.7 million individuals whom a Federal background investigation; 1.8 million referenced spouses and relatives

NIH National Institute of Allergy and Infectious Diseases

NIAID

About the Presenters

Metasebia ("Meti") Gizaw, NIAID Security Engineer

- Credentials:
  - Certified Information System Security Professional (CISSP)
  - Certified Ethical Hacker (CEH)
  - Over 12 years experience in the field
- Key Roles & Responsibilities:
  - Actively work to educate and create security awareness within project teams, and to integrate accurate levels of security for NIAID applications
  - Assist in translating security requirements and mandates from security officers that are directed to project teams; work with teams to address findings and vulnerabilities

NIH National Institute of Allergy and Infectious Diseases

*There is **no 100% secure** system or application. Effective security involves the delicate balance of reducing security risk and maintaining application functionality*

NIAID

About the Presenters

Nick Weber, NIAID Scientific Computing Project Manager

- Credentials
  - Background in science and technology; graduate degree in information management
  - Project Management Professional (PMP)
  - 6 years managing projects at NIAID
- Key Roles & Responsibilities
  - Manage and control team activities for planning, development, releases, and other aspects of (typically software development) projects
  - Document systems, submit all formal requests (procurement, change, risk, etc.)
  - Represent the project team to stakeholders

Project Case Study

NIH 3D Print Exchange: Context

Project Case Study

NIH 3D Print Exchange: Overview

Drupal™

DISCOVER SHARE CREATE LEARN ENGAGE

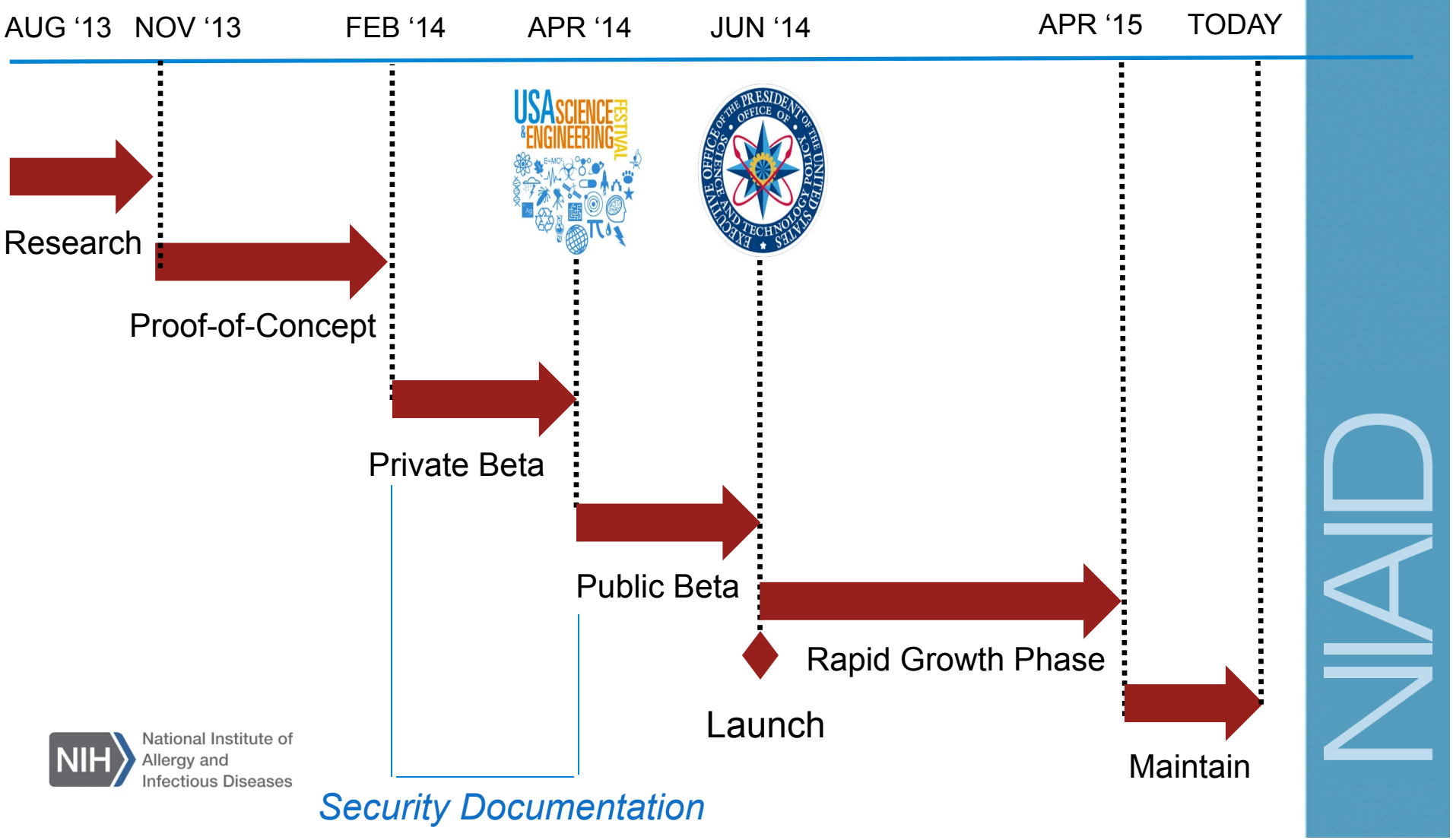
National Institute of Allergy and Infectious Diseases

NIAID


NIH 3D PRINT EXCHANGE

Project Case Study

NIH 3D Print Exchange: Schedule

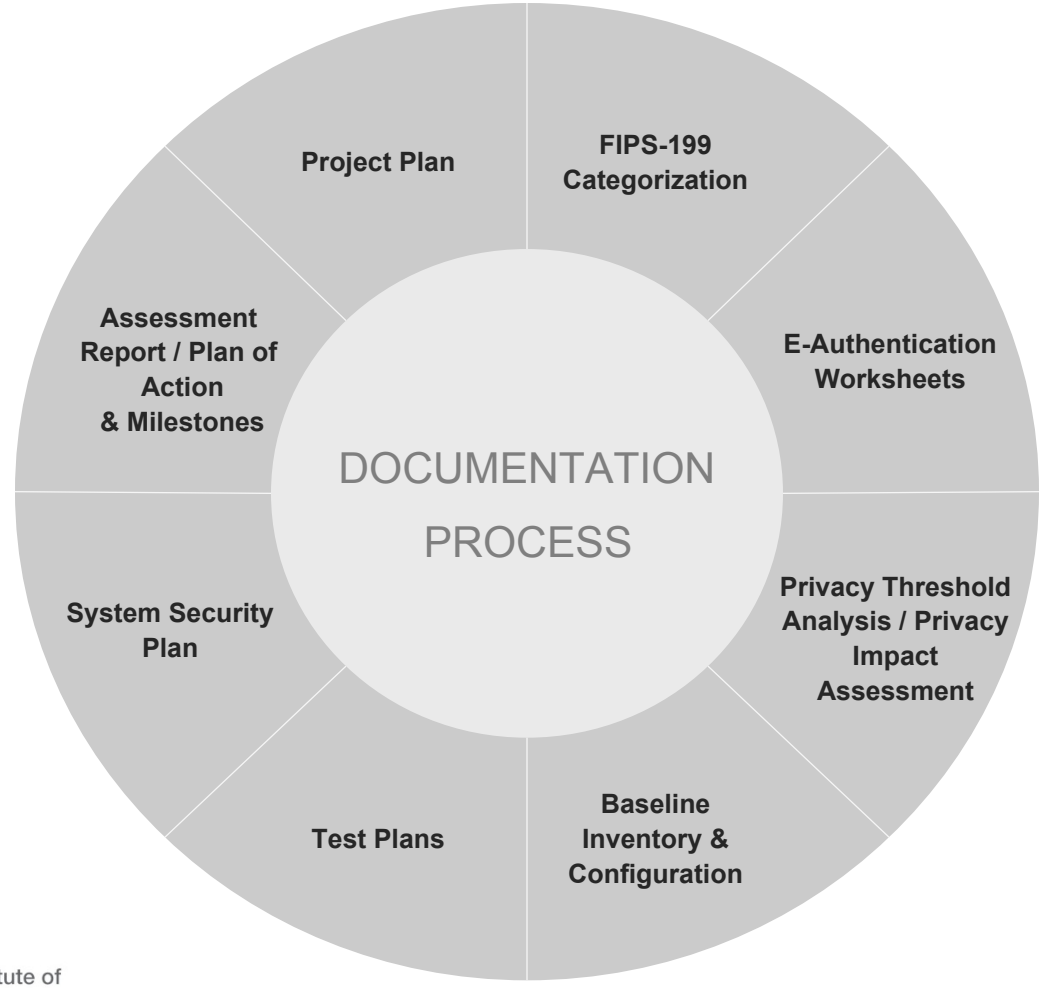


National Institute of Allergy and Infectious Diseases

NIAID

Project Case Study

NIH 3D Print Exchange: Documentation Process



National Institute of Allergy and Infectious Diseases

NIAID

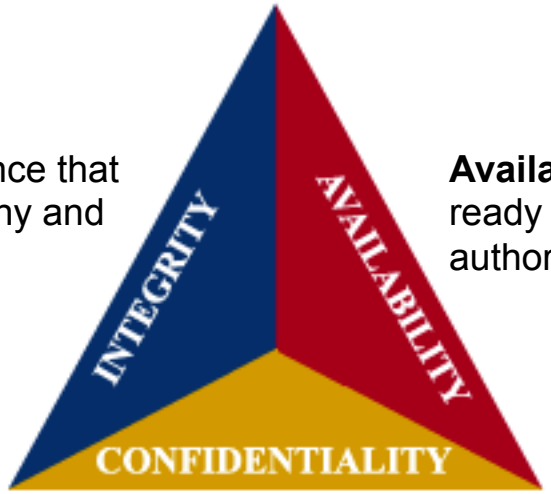
** An integrated team of people is required to create these documents*

Why secure your applications?

"Cyber War" is the new war front. NIH and government are prime targets.

- **Reduce your risk of compromise and maintain the CIA status for your application**

Integrity is the assurance that information is trustworthy and accurate



Availability is a guarantee of ready access to the information by authorized people

Confidentiality is a set of rules that limits access to information

It will cost a project team a lot more time and money to fix a finding in production than early on in the project phase

How do you secure your application?

Follow guidelines from the National Institute of Standards and Technology (NIST)

- **Select** the security controls as they apply to you your information system
- **Follow** SP (Special Publications) and FIPS PUBS (Federal Information Processing Standards Publications)
  - SP - This series reports on research, guidelines, and outreach efforts in computer security, and collaborative activities with industry, government, and academic organizations
  - FIPS PUBS - Issued by NIST after approval by the Secretary of Commerce, pursuant to Federal Information Security Management Act (FISMA) of 2002.
- **Integrate** identified security controls and standards in your lifecycle (we use the HHS Enterprise Performance Life Cycle, EPLC) to set in security in the early stages of your development process
- **Define** roles and responsibilities of management and project team members
- **Use** industry standard best practices

*Security is **<u>everyone's responsibility</u>**. Organization's security team, project management team and project developers play equal role in securing information systems.*

NIH National Institute of Allergy and Infectious Diseases

NIAID

Risk Management Framework & Process

Mapping the security authorization process to the software development life cycle

<u>Step 1</u> - Categorize the system. <u>FIPS-199</u> and <u>SP 800-60</u> publications can be used to properly identify information system overall category as High, Moderate, or Low

ILLUSTRATION BY SEGUE TECHNOLOGIES

National Institute of Allergy and Infectious Diseases

NIAID

Risk Management Framework & Process

Mapping the security authorization process to the software development life cycle

Step 2 – Select security controls. FIPS-200, SP 800-37, and SP 800-53 have information on minimum security controls for federal information systems, including guidelines on risk management and recommended security controls for different categories (High, Moderate, and Low) with corresponding controls

ILLUSTRATION BY SEGUE TECHNOLOGIES

National Institute of Allergy and Infectious Diseases

NIAID

Risk Management Framework & Process

Mapping the security authorization process to the software development life cycle

<u>Step 3</u> – Implement Security Controls. Ensure the security requirements as described in <u>SP 800-53</u> and <u>SP 800-70</u> are being addressed. Implement security checkpoints on your development lifecycle to assess progress

ILLUSTRATION BY SEGUE TECHNOLOGIES

National Institute of Allergy and Infectious Diseases

NIAID

Risk Management Framework & Process

Mapping the security authorization process to the software development life cycle

<u>Step 4</u> – Access Security Controls. Self-assessment tools and internal organization and/ or independent 3rd party assessors can be used to validate security compliance and identify risk. <u>SP 800-53 A</u> provides guideline on security assessment

ILLUSTRATION BY SEGUE TECHNOLOGIES

National Institute of Allergy and Infectious Diseases

NIAID

Risk Management Framework & Process

Mapping the security authorization process to the software development life cycle

<u>Step 5</u> – Authorize Information System. Issue an ATO (Authority To Operate) from a Authorizing Official (AO)[1] or Designated Approving Authority (DAA)[2]

1. AO: A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

2. DAA: An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.

ILLUSTRATION BY SEGUE TECHNOLOGIES

National Institute of Allergy and Infectious Diseases

NIAID

Risk Management Framework & Process

Mapping the security authorization process to the software development life cycle

<u>Step 6</u> – Monitor security controls. Continually track changes and that may affect the security posture of the information system and reassess when changed. Use automated scanning tools to scan your information system and asses risk.

ILLUSTRATION BY SEGUE TECHNOLOGIES

National Institute of Allergy and Infectious Diseases

NIAID

So what's addressed in NIST 800-53 controls?

Management, operational, & technical safeguards, broken down into 18 control families

TABLE 1-1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

What if your government system is in the cloud?

Use the Federal Risk and Authorization Management Program (FedRAMP)

- Established in December 2012
- Equivalent to FISMA controls for cloud environment
- Core concept: Authorize once, use many times
- Provides a policy for developing trusted relationship between agencies and cloud services providers (CSPs)
- CSPs are independently assessed by a Third Party Assessing Organization (3PAO) to ensure that security requirements are satisfied
- Periodic reassessment is done on the CSP to ensure their security status

NIH National Institute of Allergy and Infectious Diseases

Want some firsthand info? Talk to Shea Nangle, who gave a DrupalGovCon talk on this yesterday

BLACKMESH

NIAID

Drupal and FISMA Controls

Understand the control requirements, and leverage modules in Drupal

- The Drupal community has done the research and created shared tools and best practices on how to make applications developed in Drupal more secure
- Some work has started on applying OpenSCAP (Security Content Automation Protocol) standards
- There is no one way to address security requirements; if one solution does not work, think about compensating measures to accomplish the same level of security

NIH National Institute of Allergy and Infectious Diseases

Practice "Defense in Depth": *Attackers need only one point of entry or one door to compromise your system or data. Be sure you apply security on all levels throughout the life of your application.*

NIAID

Available Drupal Security Modules

Many modules exist; review them on Drupal.org, and test to see how they work

- **Security Review:** Automates testing for basic security checks for code execution, cross site scripting (XSS), error handling, failed logins, brute force attack
  - Addresses some of the SI (System and Information Integrity) and AC (Access Control) controls
- **Security Kit:** Provides Drupal with various security-hardening options
  - Addresses some of the SA (Systems and Services Acquisition) and SI (System and Information Integrity) controls
- **Secure Login:** Secures communication between browser and server.
  - Addresses some of the SC (System and Communication Protection) controls
- **Username Enumeration Prevention**: Prevents attacker from guessing valid usernames
  - Addresses some of the SI (System and Information Integrity) controls
- **Encrypt:** Provides the API to perform a two-way encryption
  - Addresses some of the SI (System and Information Integrity) controls
- **Permission Watchdog:** Logs all changes to permissions on roles
  - Addresses some of AU (Audit and Accountability) controls
- **Audit Logs:** Adds audit logging functionality to all entities
  - Addresses some of AU (Audit and Accountability) controls
- **Admin User by Role:**-Sets up fine-grained permissions for allowing "sub-admin" users to edit and delete other users
  - Addresses some of the AC (Access Control) controls

Available Drupal Security Modules

Many modules exist; review them on Drupal.org, and test to see how they work

…and many more!

- **CAPTCHA/reCAPTCHA**: Challenge-response test most often placed within web forms and reCAPTCHA protects emails
- **Honeypot:** Applies honeypot and timestamp methods of deterring spam bots from completing forms on Drupal sites
- **Auto Logout**: Provides a site administrator the ability to log users out after a specified time of inactivity
- **ClamAV**: Verifies that files uploaded to a site are not infected with a virus, and prevents infected files from being saved

Use automated tools to validate systems

Practice validation yourself using available tools, before validation by auditors

Static Code Analysis

- SAST – Static Application Security Tools are used to scan source code or the binary code of an application
  - This allows codes to be tested in small units as the application is developed
  - There are several tools that are recommended by Gartner, including ones from HP, IBM, and Veracode

Dynamic Code Analysis

- DAST – Dynamic Application Security Tools are used to test an application in its running state
  - This simulates web traffic and crawls the application while it's running
  - There are several tools that are recommended by Gartner, including ones from HP, IBM, and Checkmarx

If you are expecting high traffic to your application, use a load testing tool to determine the capacity of your environment. We used cloud based tool, LoadStorm, for our public-facing Drupal website.

Why do all of this?

Remember that security is everyone's responsibility, not just that of security officers

- Key benefits:
  - Enables a more secure system, and likely one that is secure enough to deter the common hacker looking for a challenge
  - Frees up resource time in the long run, enabling teams to focus on improvements and other projects
  - Identifies vulnerabilities in other systems, thereby increases overall security awareness
  - Saves money (and reduces stress) on bug fixes for if/when security vulnerabilities are detected

Closing Thought

If it takes Ethan Hunt to compromise to your data, you've done your job!

Top Ten Take-Aways from a Project Manager

What have I learned from working through this process?

1. DON'T (FULLY) DELEGATE THIS TASK
2. START AS EARLY AS POSSIBLE; BAKE IN, DON'T BOLT ON
3. KEEP ASKING QUESTIONS AND LOOKING FOR WHAT YOU CAN RE-APPLY
4. "THERE'S A MODULE FOR THAT!" (PROBABLY)
5. DOCUMENT, DOCUMENT, DOCUMENT
6. PROACTIVELY SCAN YOUR APPLICATION
7. CLEAN UP AFTER YOURSELF
8. UNDERSTAND THAT THIS ALL BOILS DOWN TO RISK ACCEPTANCE
9. AVOID HAVING AN "US VS. THEM" MENTALITY ABOUT SECURITY AAUDITS / AUDITORS
10. EXPECT TO HEAR "NO"; DON'T BE AFRAID TO CHALLENGE UNDERLYING ASSUMPTIONS

NIAID

Top ~~Ten~~ Eleven Take-Aways from a Project Manager

What have I learned from working through this process?

11 FIND A WAY TO GET ACCESS TO SOMEONE LIKE METI!

NIAID

Acknowledgements

We owe a big "Thank You!" to a ton of people

- National Institute of Allergy and Infectious Diseases (NIAID)
  - NIH 3D Print Exchange Team
  - NIAID Cyber Security Program
  - Office of Cyber Infrastructure & Computational Biology (OCICB) Management and Operations Teams
- Department of Health and Human Services (HHS)
- Squishymedia
- NIH Library & DrupalGovCon
- *The list goes on…*

NIH National Institute of Allergy and Infectious Diseases

NIAID

Questions?

(Sorry, our Drupal expert is under the weather…)

National Institute of Allergy and Infectious Diseases

NIAID

References

(These correspond to underlined areas in prior slides)

- http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
- https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf
- http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0
- http://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story/
- http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html#page=1
- http://www.nist.gov/
- http://csrc.nist.gov/publications/PubsSPs.html
- http://csrc.nist.gov/publications/PubsFIPS.html
- https://events.drupal.org/losangeles2015/bofs/drupal-and-fisma-compliance
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf
- http://loadstorm.com/