UCAR

COSMIC

FISMA

Lions and Tigers

Jose Castilleja, ISSO
Susan Ramsey, ISA, RE
Dr. G. Robert Williams, CO

Open Computing, Open Network, Open Data

UCAR's mission is to empower our Member Institutions, our National Center, and our Community Programs by

- *Promoting research excellence*
- *Developing fruitful collaborations*
- *Managing unique resources*
- *Creating novel capabilities*
- *Building critical applications*
- *Expanding educational opportunities*
- *Engaging in effective advocacy*

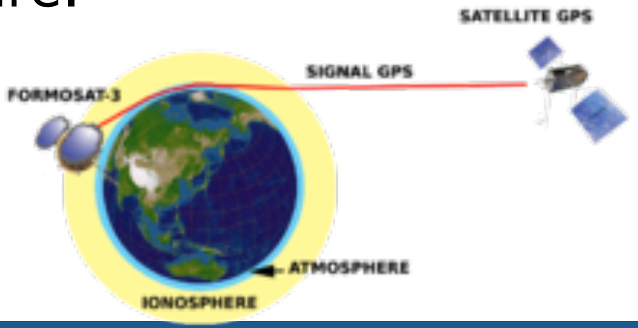
← Nothing in here mentions FISMA

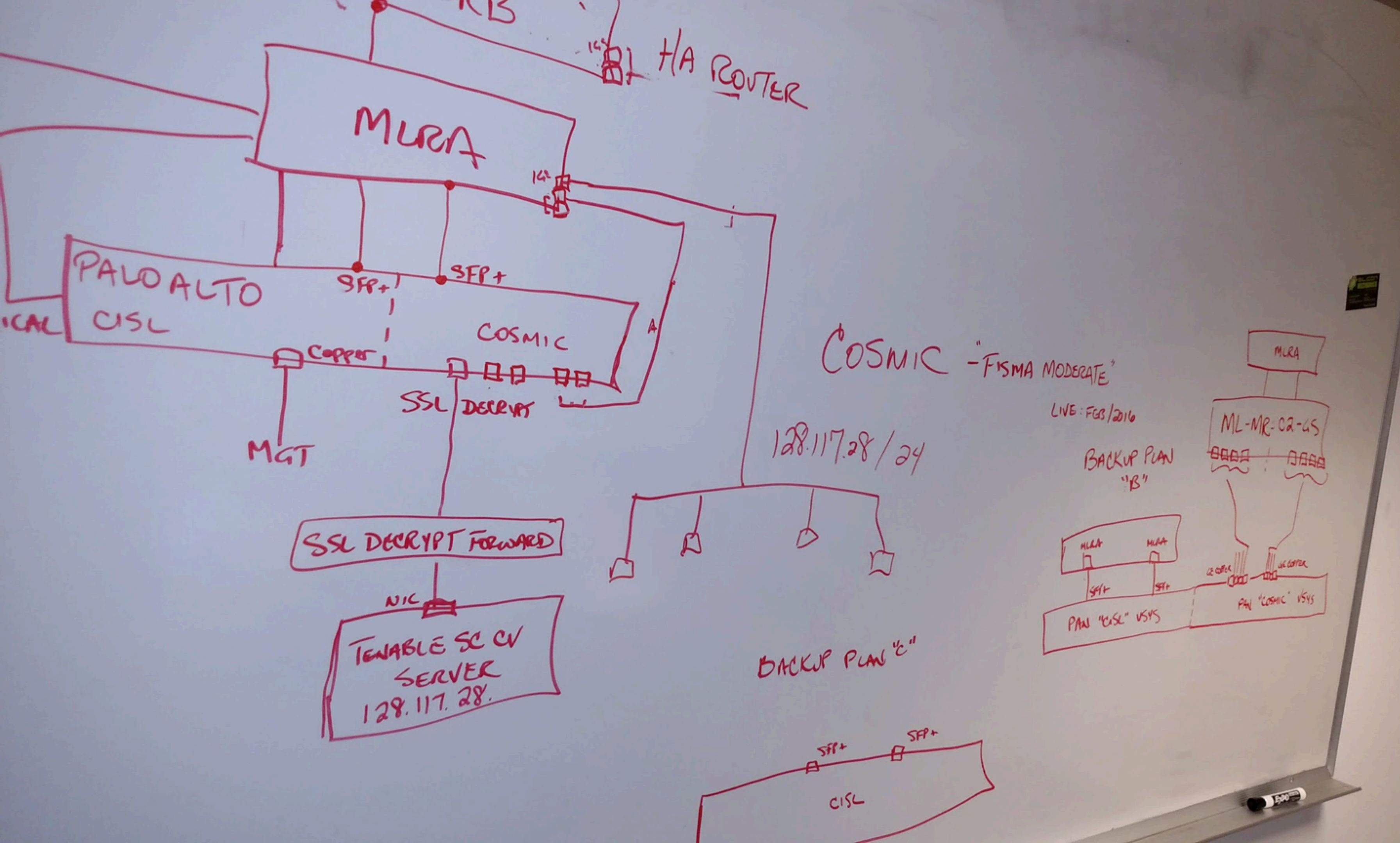
NCAR's mission is

- *to understand the behavior of the atmosphere and related Earth and geospace systems*
- *to support, enhance, and extend the capabilities of the university community and the broader scientific community, nationally and internationally, and*
- *to foster the transfer of knowledge and technology for the betterment of life on Earth*

Enter the COSMIC-P/GD

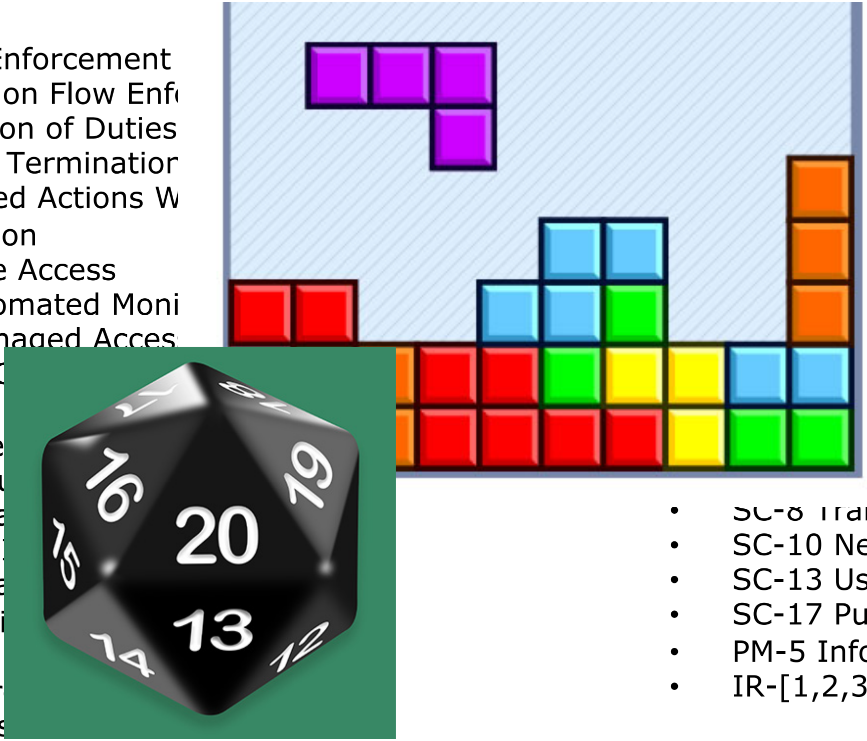
COSMIC is a Community Division at NCAR that is funded by various organizations to process satellite data using **radio occultation** computation. I can't pretend to explain this, but they measure the way radio waves bend as they enter the atmosphere, and then they calculate amazing things based on how bendy they are.




RB
1G
H/A ROUTER
MLRA
1G
PALO ALTO
CISL
ICAL
SFP+
SFP+
COSMIC
A
Copper
MGT
SSL DECRYPT
SSL DECRYPT FORWARD
NIC
TENABLE SC CV
SERVER
128.117.28.
128.117.28 / 24
COSMIC - "FISMA MODERATE"
LIVE: FEB/2016
BACKUP PLAN
"B"
MLRA
ML-MR-C2-GS
MLRA
MLRA
SFP+
SFP+
C2 COPPER
GS COPPER
PAN "CISL" VSYS
PAN "COSMIC" VSYS
BACKUP PLAN "C"
SFP+
SFP+
CISL

Boundary Protection and…

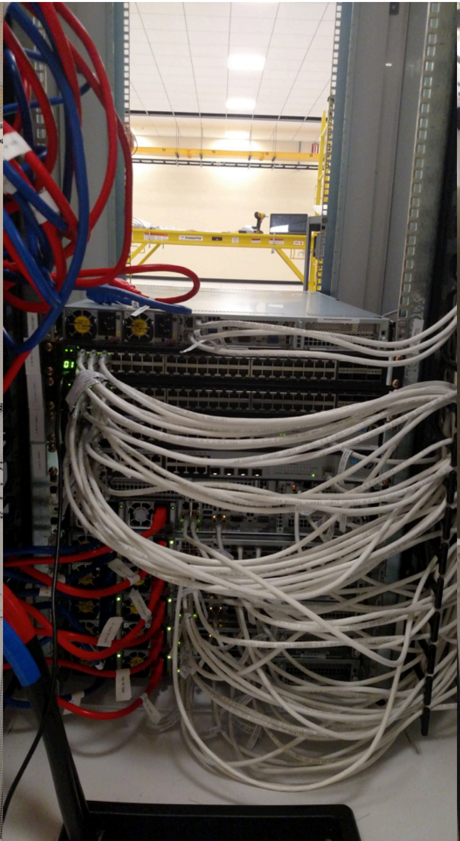
- AC-3 Access Enforcement
- AC-4 Information Flow Enf
- AC-5 Separation of Duties
- AC-12 Session Terminatior
- AC-14 Permitted Actions W
  or Authentication
- AC-17 Remote Access
- AC-17 (1) Automated Moni
- AC-17 (3) Managed Acces
- AC-19 Access C
- AC-22 Publicly
- RA-3 Risk Asse
- CA-7 Continuou
- CM-3 Configura
- CM-4 Security
- CM-6 Configura
- CM-8 Informati
  Inventory
- CM-10 Softwar
- CM-11 User Ins



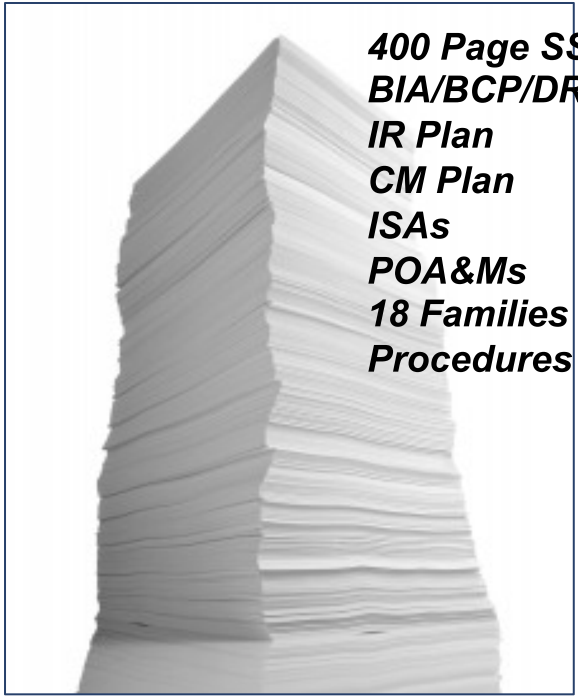
y Maintenance
emediation
us Code Protection
ation Systems Monitoring
ty Alerts, Advisories and Directives
ote Access
able Events
udit Review and Reporting
Identification and Authentication
graphic Module Authentication
l of Service Protection
lary Protection

- SC-8 Transmission Confidentiality and Integrity
- SC-10 Network Disconnect
- SC-13 Use of Cryptography
- SC-17 Public Key Infrastructure Certificates
- PM-5 Information System Inventory
- IR-[1,2,3,4,5,6,7,8] Incident Response All

The Fun Part

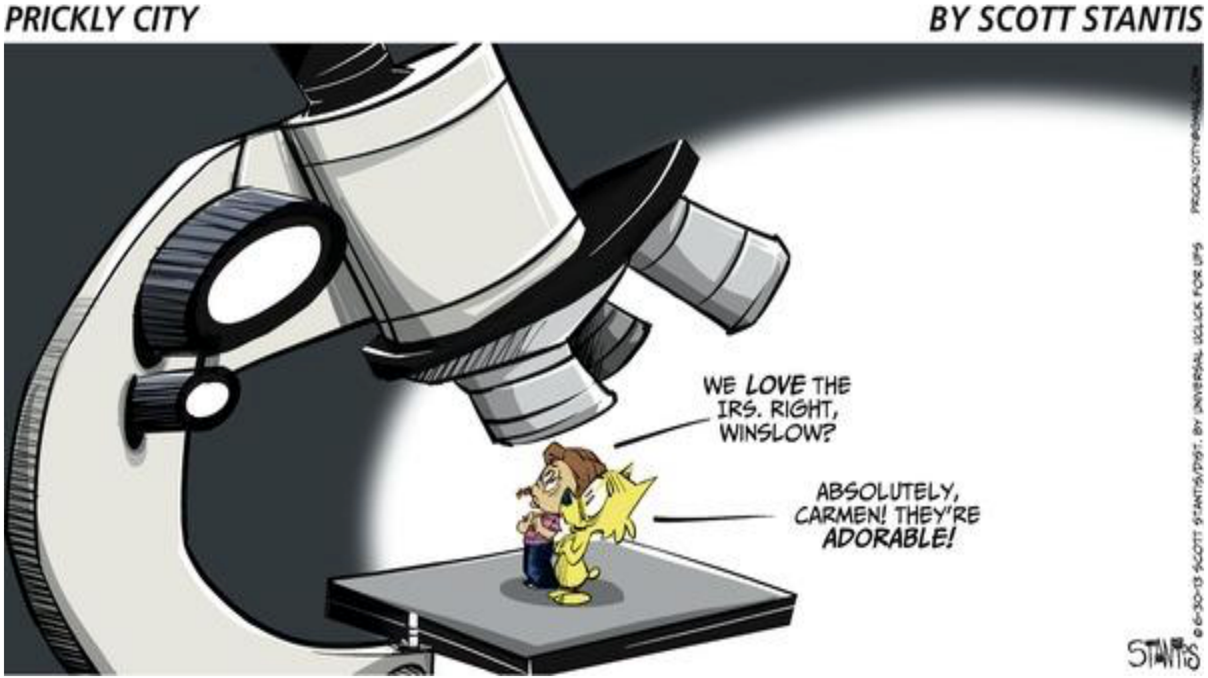


The Hard Part



400 Page SSP
BIA/BCP/DR Plans
IR Plan
CM Plan
ISAs
POA&Ms
18 Families of Policies and Procedures

External Assessment


PRICKLY CITY
BY SCOTT STANTIS
WE *LOVE* THE IRS. RIGHT, WINSLOW?
ABSOLUTELY, CARMEN! THEY'RE *ADORABLE!*
STANTIS
© 6-30-13 SCOTT STANTIS/DIST. BY UNIVERSAL UCLICK FOR UFS
PRICKLYCITY@

1. Really Document Your System

- Asset Inventory
- Service/Port Inventory
- Software Inventory
- Baseline Configuration
- Audit Metrics, and Why You Collect Them
- Man man – just print it out

2. Get Executive Sponsorship

- Set expectations
- Change management
- **Conflict management**

“...you’re taking away my creativity!!”

“...I can’t be root any more?”

“You mean I have to file a ticket to open a port on the firewall????”

3. Build a Solid Team

- Hire a fearless FISMA Consultant
- Hire or borrow a technical writer, or three
- Select teammates with integrity
- … and stamina
- … and a sense of humor

👌♏ ■♓♍♏ □❐ ⌧□◆❒ 💧💧⚐ ⬥♓●
⬧◆♌❍♓⧫⧫♏♎≏
✋■ ⌖♓■♑☟♓■♑⬧

4. Pull Your Executives Into the Audit

Lie.
Make them sign Official Documents.
Tell them you have donuts. Or Starbucks.

Just get them involved.

5. Negotiate the Scope of Your SSP

Categorize

SELECT

Implement

Assess

Authorize

Monitor

When NIST says "select", they mean "select". "Tailor Out" as as much as you can. Practice saying "That control is out of scope for this audit."

6. Read Not Just 800-53, but 800-53a

Practice the audit questions. We got dinged on XX-01 on every control family because although we "disseminated" all the policies, we did not have it explicitly documented **how** the organization disseminated the policies, nor who was responsible for said dissemination.

Really! We disseminate by carrier pigeon!!!!

7. Negotiate the Scope of Your SAP

Our fearless Compliance
Officer saved our bacon on this one.

We wanted different colors.
And we hate pie charts.
No pie charts.

8. Don’t Distract the Auditors

A 400-page SSP is really boring, especially when you’ve read ¾ of it a dozen times. I joked and laughed and had a good time during the audit interviews. I’m pretty sure it backfired in that they forgot to record some pieces of evidence. This meant we had to basically conduct the interviews again.

Keep the auditors on task, politely and firmly

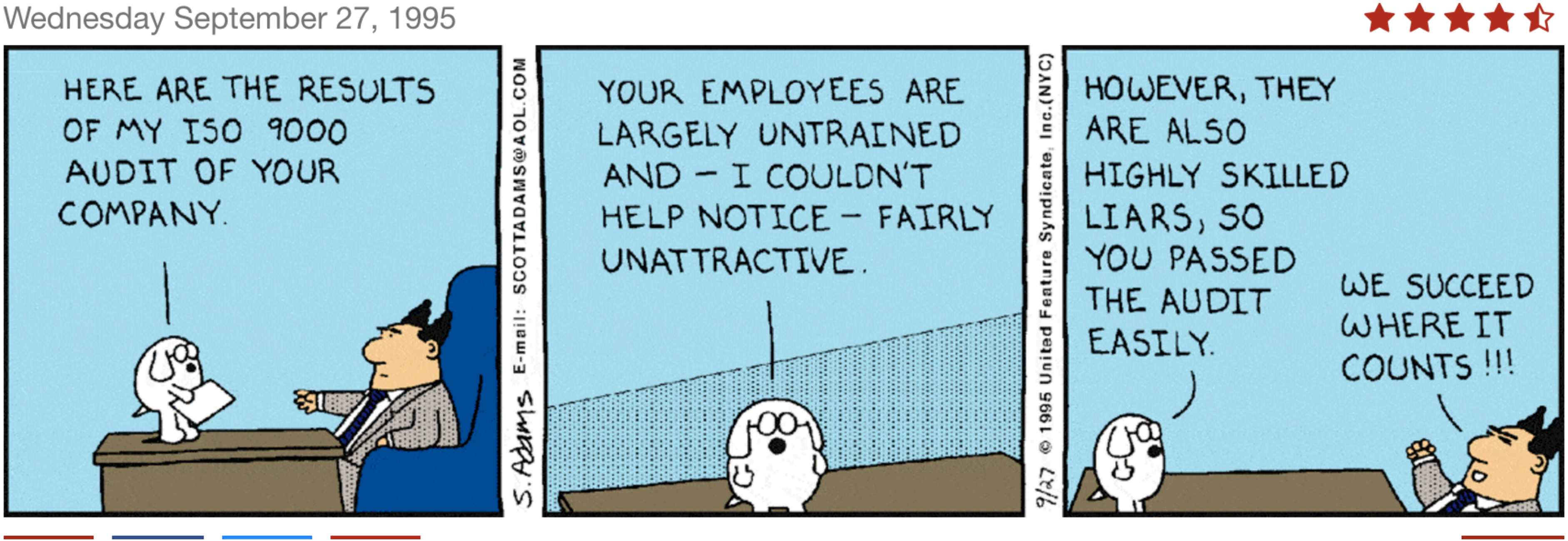
Look!!! Squirrel!!!

9. Negotiate Your SAR

At least try talking them down…high to moderate…moderate to low….

I SUGGEST WE ACCEPT THAT THE PUNCTUATION ON PAGE 26 COULD HAVE BEEN BETTER
MAYBE WE SHOULD JUST CONCEDE THE SEMI COLON!
GIVE THEM THE SEMI COLON AND THEY'LL REJECT THE WHOLE DAMN CONTRACT!

10. Compliance is Not Security


Wednesday September 27, 1995
HERE ARE THE RESULTS OF MY ISO 9000 AUDIT OF YOUR COMPANY.
S. Adams E-mail: SCOTTADAMS@AOL.COM
YOUR EMPLOYEES ARE LARGELY UNTRAINED AND – I COULDN'T HELP NOTICE – FAIRLY UNATTRACTIVE.
9/27 © 1995 United Feature Syndicate, Inc.(NYC)
HOWEVER, THEY ARE ALSO HIGHLY SKILLED LIARS, SO YOU PASSED THE AUDIT EASILY.
WE SUCCEED WHERE IT COUNTS !!!

Because I Know You Want the Tech Stack

Base Platform:

- 20 servers
- 4 Brocade switches
- 2 Palo Alto 3060/5060 NFWs
- Silicon Mechanics HW
- CentOS 6
- KVM

Staff Count: 1.75

Continuous Monitoring:

- Tenable Security Center (Nessus, Log Correlation Engine)
- Nagios
- ClamAV
- Cron
- Palo Alto Application and Threat
- Palo Alto URL Filtering

Configuration Management:

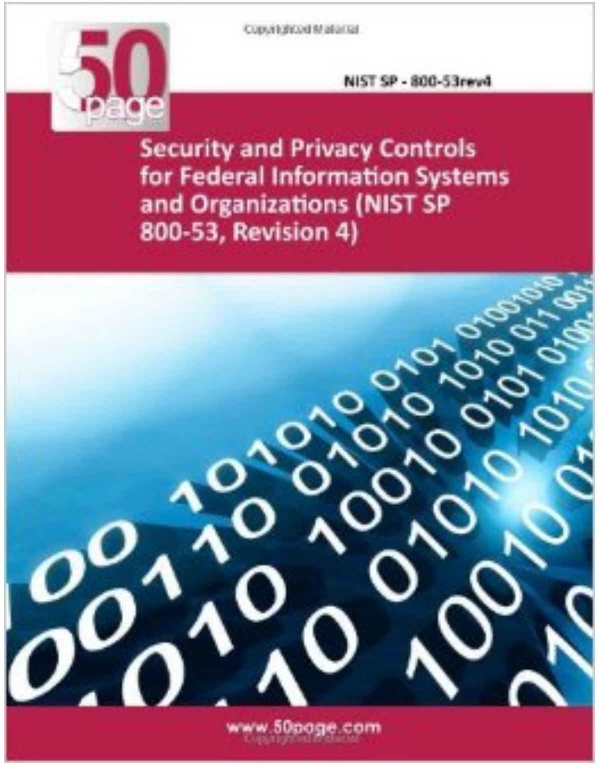
- Puppet
- Subversion
- Redmine

Seriously

Yes, there is room to improve things. Regardless, 800-53 is totally worth the read.

Where we go from here:

- All UCAR FISMA “Low”
- RMF
- Continuous Monitoring



Copyrighted Material

50 page

NIST SP - 800-53rev4

Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53, Revision 4)

www.50page.com

Copyrighted Material

How I learned to stop worrying and love

HIPAA

And So Can You

Anurag Shankar, Center for Applied Cybersecurity Research, Indiana University

2000: Lilly Foundation funds the Indiana Genomics Initiative (INGEN). The Research Computing division at Indiana University (which is part of IU’s central IT shop) is tasked with empowering genomics research at the School of Medicine.

2000: Yours truly goes out to hawk IU’s advanced cyberinfrastructure to the doctors.

There are no takers. Why? HIPAA.

When they ask “Are you HIPAA compliant?” we don’t know. So they don’t come.

Things simmer and cook.

2007: The management decides to build it so they will come.

A HIPAA project is launched.

2008: Yours truly is tasked with figuring it all out.

There are no peers to be found.
I go try to learn what I can.

HIPPA

HIPAA

- **Health** Information Privacy Protection Act

- **Health** Insurance Portability and Accountability Act

It's about the ability to take your health insurance with you when you change jobs.

2008: HIPAA says to manage risk using reasonable and appropriate safeguards consistent with resources available. The safeguards are broadly defined to be flexible.

Well, this seemed quite reasonable.

2008: The task at hand is no less than to make our entire research cyberinfrastructure HIPAA compliant.

How to go about it?

Question #1: Who should be involved?

= everyone who may complain later that we didn’t do it right.

= Central IT management and administrators, Counsel, University HIPAA compliance office, Internal Audit, School of Medicine CIO, faculty, IT staff

We put them on an oversight committee - wisest move we ever made.

2008: Came up with a homegrown, HIPAA-specific process, involving risk management and a LOT of documentation. Took 1.0 FTE for a year (initial effort), 0.25 for ongoing.

2009: We were deemed "capable of handling PHI".

2012: Other rules and regs began to appear on the horizon, e.g. FISMA, as well as many other central IT systems needing compliance.

HIPAA specificity had to go.

2013: Developed a comprehensive, NIST based risk management framework to simultaneously handle HIPAA and FISMA.

Still in use. Happy to provide consulting and templates.

2016: After nearly a decade of HIPAA-natizing later, what are my thoughts?

HIPAA is eminently doable. In fact, you are doing (most of) it already.

HIPAA Humor (North Dakota Dept of Health)

- □ HIPAA-Ectomy - the removal of individual identifiable health information from records
- □ HIPAA-Glycemia – a low level of understanding of the HIPAA regulations
- □ HIPAA-Phobia – a morbid fear of HIPAA regulations
- □ HIPAA-Thermia – the unexplained chill that is running down the back of anyone associated with HIPAA