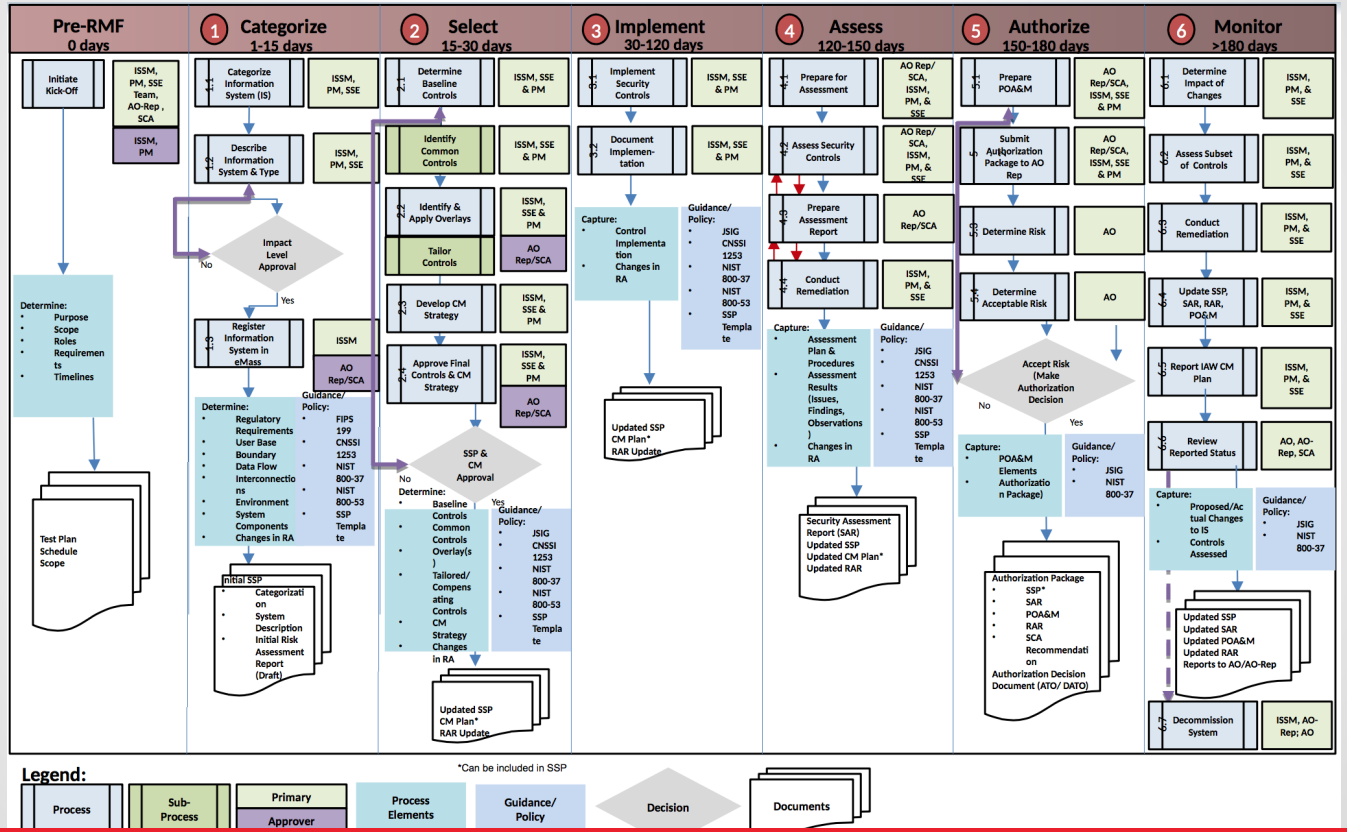
Security & Scanning

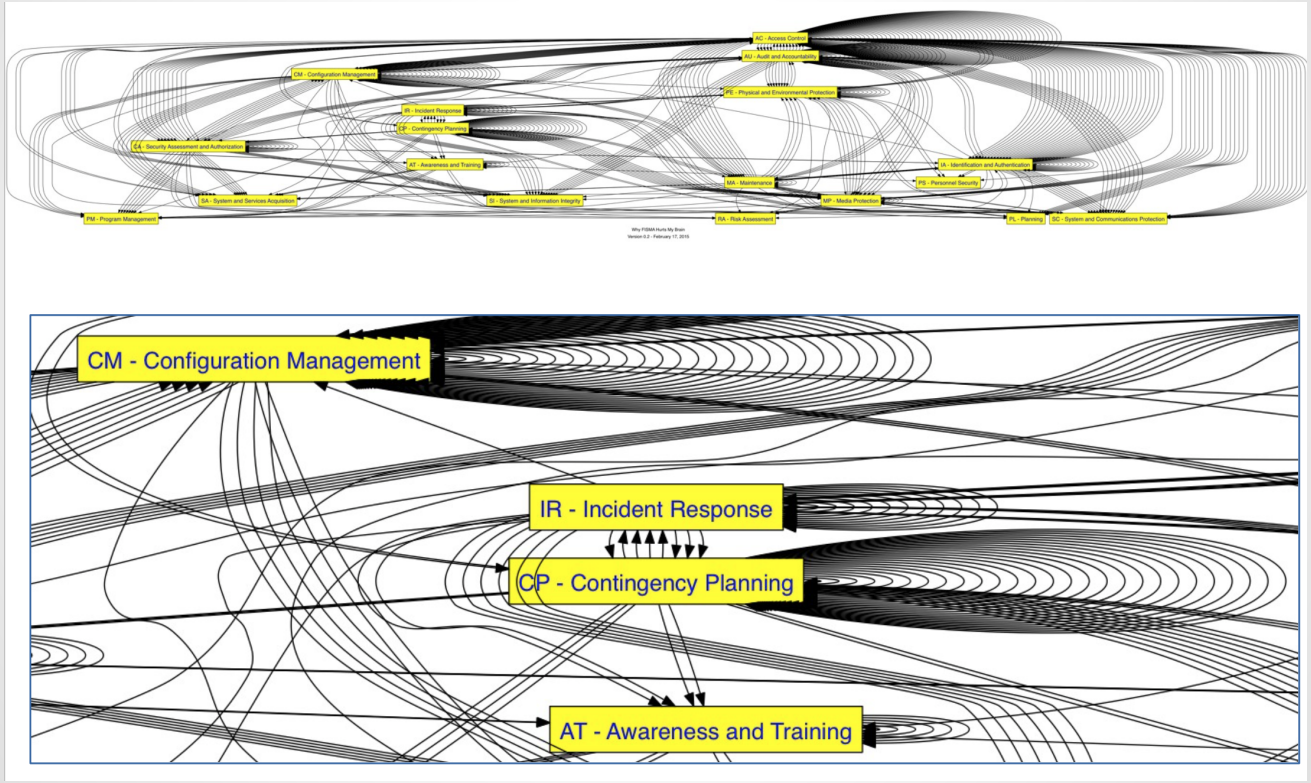
An Open Source Approach

Explaining FISMA

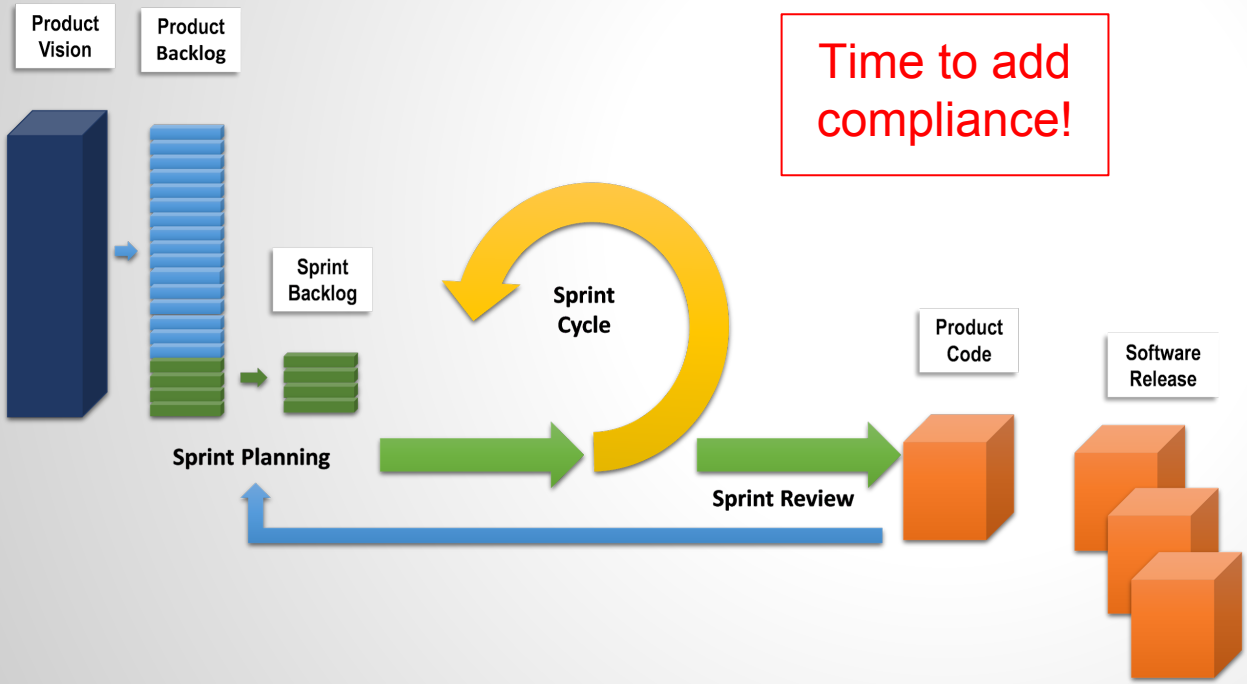
NIST Risk Mgt Framework Takes Months



NIST 800-53 Controls Hurt Your Brain



Software Supply Chain Can Aid Security



Time to add compliance!

10 deploys per day

Dev & ops cooperation at Flickr

John Allspaw & Paul Hammond

Velocity 2009

source Gene Kim

FISMA for Happy Developers

```
$ risk -a server.agency.gov
$ make artifact=system-security-plan -f doc
```

Scanning as Part of CI

Problem

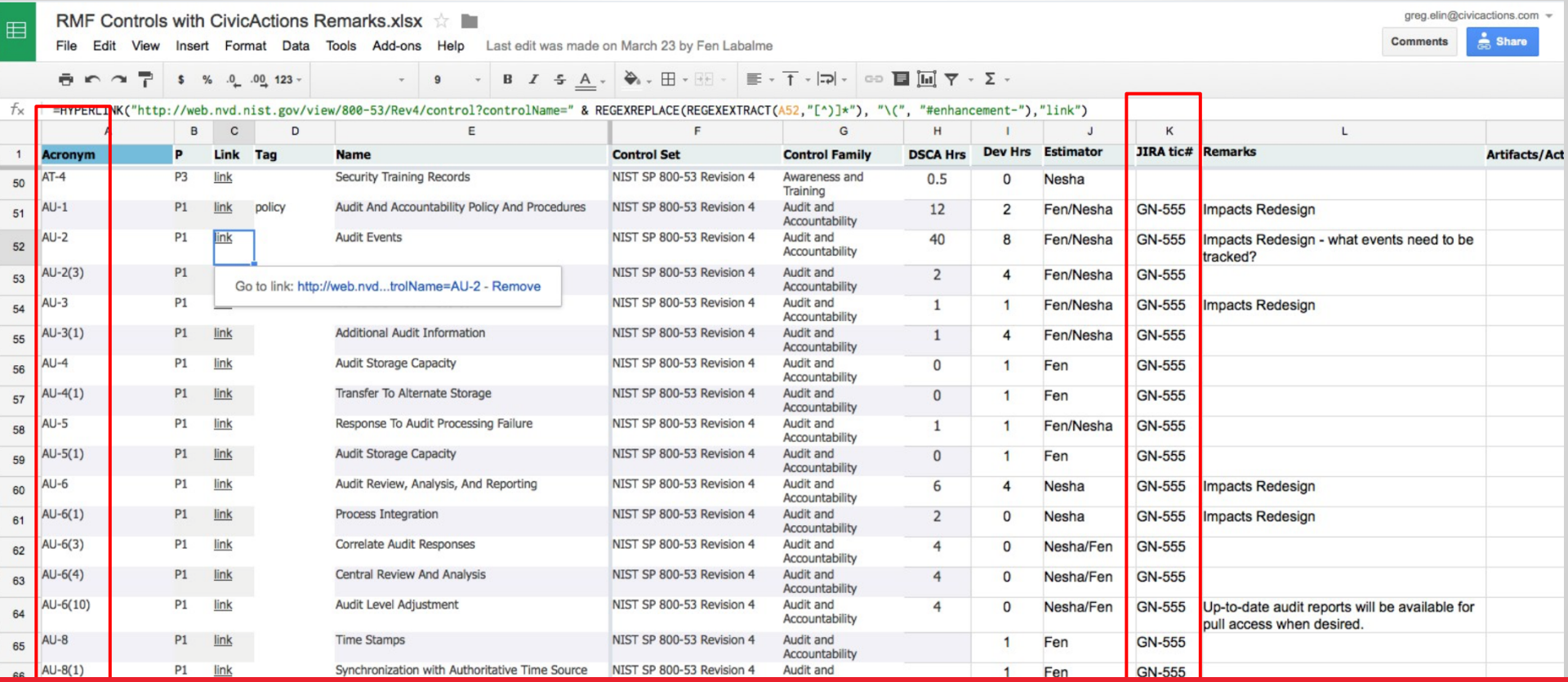
Developers reaction to security scans

Tip #1: Use the Families

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessments 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 Service Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

“Use the families, Luke.”

Tip #2: Give Control Families Tickets



RMF Controls with CivicActions Remarks.xlsx

File Edit View Insert Format Data Tools Add-ons Help Last edit was made on March 23 by Fen Labalme

greg.elin@civicactions.com

Comments Share

=HYPERLINK("http://web.nvd.nist.gov/view/800-53/Rev4/control?controlName=" & REGEXREPLACE(REGEXEXTRACT(A52,"[^)]*"), "\(", "#enhancement-"),"link")

Go to link: http://web.nvd...trolName=AU-2 - Remove

	A	B	C	D	E	F	G	H	I	J	K	L	
1	Acronym	P	Link	Tag	Name	Control Set	Control Family	DSCA Hrs	Dev Hrs	Estimator	JIRA tic#	Remarks	Artifacts/Act
50	AT-4	P3	link		Security Training Records	NIST SP 800-53 Revision 4	Awareness and Training	0.5	0	Nesha			
51	AU-1	P1	link	policy	Audit And Accountability Policy And Procedures	NIST SP 800-53 Revision 4	Audit and Accountability	12	2	Fen/Nesha	GN-555	Impacts Redesign	
52	AU-2	P1	link		Audit Events	NIST SP 800-53 Revision 4	Audit and Accountability	40	8	Fen/Nesha	GN-555	Impacts Redesign - what events need to be tracked?	
53	AU-2(3)	P1				NIST SP 800-53 Revision 4	Audit and Accountability	2	4	Fen/Nesha	GN-555		
54	AU-3	P1				NIST SP 800-53 Revision 4	Audit and Accountability	1	1	Fen/Nesha	GN-555	Impacts Redesign	
55	AU-3(1)	P1	link		Additional Audit Information	NIST SP 800-53 Revision 4	Audit and Accountability	1	4	Fen/Nesha	GN-555		
56	AU-4	P1	link		Audit Storage Capacity	NIST SP 800-53 Revision 4	Audit and Accountability	0	1	Fen	GN-555		
57	AU-4(1)	P1	link		Transfer To Alternate Storage	NIST SP 800-53 Revision 4	Audit and Accountability	0	1	Fen	GN-555		
58	AU-5	P1	link		Response To Audit Processing Failure	NIST SP 800-53 Revision 4	Audit and Accountability	1	1	Fen/Nesha	GN-555		
59	AU-5(1)	P1	link		Audit Storage Capacity	NIST SP 800-53 Revision 4	Audit and Accountability	0	1	Fen	GN-555		
60	AU-6	P1	link		Audit Review, Analysis, And Reporting	NIST SP 800-53 Revision 4	Audit and Accountability	6	4	Nesha	GN-555	Impacts Redesign	
61	AU-6(1)	P1	link		Process Integration	NIST SP 800-53 Revision 4	Audit and Accountability	2	0	Nesha	GN-555	Impacts Redesign	
62	AU-6(3)	P1	link		Correlate Audit Responses	NIST SP 800-53 Revision 4	Audit and Accountability	4	0	Nesha/Fen	GN-555		
63	AU-6(4)	P1	link		Central Review And Analysis	NIST SP 800-53 Revision 4	Audit and Accountability	4	0	Nesha/Fen	GN-555		
64	AU-6(10)	P1	link		Audit Level Adjustment	NIST SP 800-53 Revision 4	Audit and Accountability	4	0	Nesha/Fen	GN-555	Up-to-date audit reports will be available for pull access when desired.	
65	AU-8	P1	link		Time Stamps	NIST SP 800-53 Revision 4	Audit and Accountability		1	Fen	GN-555		
66	AU-8(1)	P1	link		Synchronization with Authoritative Time Source	NIST SP 800-53 Revision 4	Audit and		1	Fen	GN-555		

Tip #3: Use SCAP


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-117

Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0

SCAP == Shared Unit Testing for Vulnerabilities

Vulnerabilities

- Poor configuration
- Known exploits

Tip #4: Use OpenSCAP + GovReady

Community created portfolio of tools and content to make attestations about known vulnerabilities

https://github.com/OpenSCAP

Open source tool that to make OpenSCAP scanning friendlier to developers

https://github.com/GovReady/govready

OpenSCAP

```
$ oscap xccdf eval --remediate \
--profile stig-rhel6-server-upstream \
--report /root/scan-report.html \
/usr/share/xml/scap/content.xml
```

GovReady

```
$ govready scan
$ govready fix
$ govready compare
```

Next steps

- Include more operating systems (Ubuntu, Debian)
- Add more tests (bash & drush based)
- Create and contribute towards an application baseline:
  - Drupal
  - Apache/Nginx
  - MySQL/Mariadb

Branch: **drupal** ansible-scap / roles / drupal-security / tasks / **main.yml**

openprivacy 20 hours ago Add some security modules

1 contributor

52 lines (46 sloc) | 1.983 kB

Raw Blame History

```
---

- name: Install and enable some Drupal security modules.
  command: >
    /usr/local/bin/drush en -y {{ drupal_security_modules }}
    chdir={{ drupal_core_path }}
    creates={{ drupal_core_path }}/sites/all/modules/autologout

- name: autologout - AC-3 Access Enforcement (see Organization Policy AC-2(5) Inactivity Logout)
  command: >
    /usr/local/bin/drush vset {{ item }}
    chdir={{ drupal_core_path }}
  with_items:
    - autologout_redirect_url '/'
    - autologout_enforce_admin 1
    - autologout_role_2 1
    - autologout_role_2_timeout 3600
    - autologout_role_9 1
    - autologout_role_9_timeout 3600
    - autologout_role_logout 1
    - autologout_timeout 3600
    - autologout_use_watchdog 1

- name: session_limit - AC-3 Access Enforcement (Session limits)
  command: >
    /usr/local/bin/drush vset {{ item }}
    chdir={{ drupal_core_path }}
  with_items:
    - session_limit_logged_out_message 'You have been automatically logged out. Someone else has logged in with your u
    - session_limit_logged_out_message_severity 'error'
    - session_limit_max 1
```

```
± [fen@truckin] ~/workspace/security/ansible-scap 4ff21d5|drupal ✓
» ansible-playbook -i inventory -u vagrant -l server drupal-security.yml

PLAY [Ensure that security modules are present, enabled and configured.] ******

GATHERING FACTS ***************************************************************
ok: [server]

TASK: [drupal-security | Install and enable some Drupal security modules.] ****
ok: [server]

TASK: [drupal-security | autologout - AC-3 Access Enforcement (see Organization Policy AC-2(5) Inactivity Logout)] ***
changed: [server] => (item=autologout_redirect_url '/')
changed: [server] => (item=autologout_enforce_admin 1)
changed: [server] => (item=autologout_role_2 1)
changed: [server] => (item=autologout_role_2_timeout 3600)
changed: [server] => (item=autologout_role_9 1)
changed: [server] => (item=autologout_role_9_timeout 3600)
changed: [server] => (item=autologout_role_logout 1)
changed: [server] => (item=autologout_timeout 3600)
changed: [server] => (item=autologout_use_watchdog 1)

TASK: [drupal-security | session_limit - AC-3 Access Enforcement (Session limits)] ***
changed: [server] => (item=session_limit_logged_out_message 'You have been automatically logged out. Someone else has logged in with your username and passwor
d and the maximum number of @number simultaneous sessions was exceeded. This may indicate that your account has been compromised or that account sharing is no
t allowed on this site. Please contact the site administrator if you suspect your account has been compromised.')
changed: [server] => (item=session_limit_logged_out_message_severity 'error')
changed: [server] => (item=session_limit_max 1)

TASK: [drupal-security | ejector_seat - AC-3 Access Enforcement (Session limits)] ***
changed: [server] => (item=ejectorseat_background 0)
changed: [server] => (item=ejectorseat_interval 120)

TASK: [drupal-security | flood_control - AC-7 Unsuccessful Logon Attempts] ****
changed: [server] => (item=user_failed_login_ip_limit 50)
changed: [server] => (item=user_failed_login_ip_window 3600)
changed: [server] => (item=user_failed_login_user_limit 4)
changed: [server] => (item=user_failed_login_user_window 1800)
changed: [server] => (item=contact_threshold_limit 5)
changed: [server] => (item=contact_threshold_window 3600)

PLAY RECAP ********************************************************************
server                     : ok=6    changed=4    unreachable=0    failed=0


± [fen@truckin] ~/workspace/security/ansible-scap 4ff21d5|drupal ✓
»
```

HOW TO ENGAGE

OpenSCAP GitHub:
https://github.com/OpenSCAP

NIST SCAP Website:
https://scap.nist.gov

OpenSCAP References & Docs:
https://github.com/OpenSCAP/scap-security-guide/wiki/Collateral-and-References

SCAP Content Mailing List:
https://fedorahosted.org/mailman/listinfo/scap-security-guide

GovReady user-friendly front-end:
https://github.com/GovReady/govready

Ansible-SCAP demo. See how it all works on the “drupal” branch - painlessly:
https://github.com/openprivacy/ansible-scap

CONTACT INFO

Fen Labalme
fen@civicactions.com
412-996-4113

Greg Elin
gregelin@gitmachines.com
917-304-3488