RED HAT
SUMMIT

LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.

June 11-14, 2013
Boston, MA

RED HAT
SUMMIT

COMPLIANCE MADE EASY

Shawn Wells
Director, Innovation Programs
12-JUNE-2013

shawn@redhat.com | @shawndwells

50 MINUTES, 3 GOALS

1. Review security compliance tech + initiatives
   - SCAP Security Guide Project
   - Security Technical Implementation Guides (STIGs)
   - FedRAMP / FISMA Moderate

2.

3.

50 MINUTES, 3 GOALS

1. Review security compliance tech + initiatives
   - SCAP Security Guide Project
   - Security Technical Implementation Guides (STIGs)
   - FedRAMP / FISMA Moderate
2. Demonstrate current capabilities
   - OpenSCAP + SCAP Security Guide [CLI]
   - RHN Satellite Audit [GUI]
3.

50 MINUTES, 3 GOALS

1. Review security compliance tech + initiatives
   - SCAP Security Guide Project
   - Security Technical Implementation Guides (STIGs)
   - FedRAMP / FISMA Moderate

2. Demonstrate current capabilities
   - OpenSCAP + SCAP Security Guide [CLI]
   - RHN Satellite Audit [GUI]

3. Discuss compliance content roadmap
   - Program validation & priority adjustment

FIRST: WHAT'S THE PROBLEM?

RHEL5 STIG (U.S. Military Baseline)

- 587 compliance items
- Many are manual

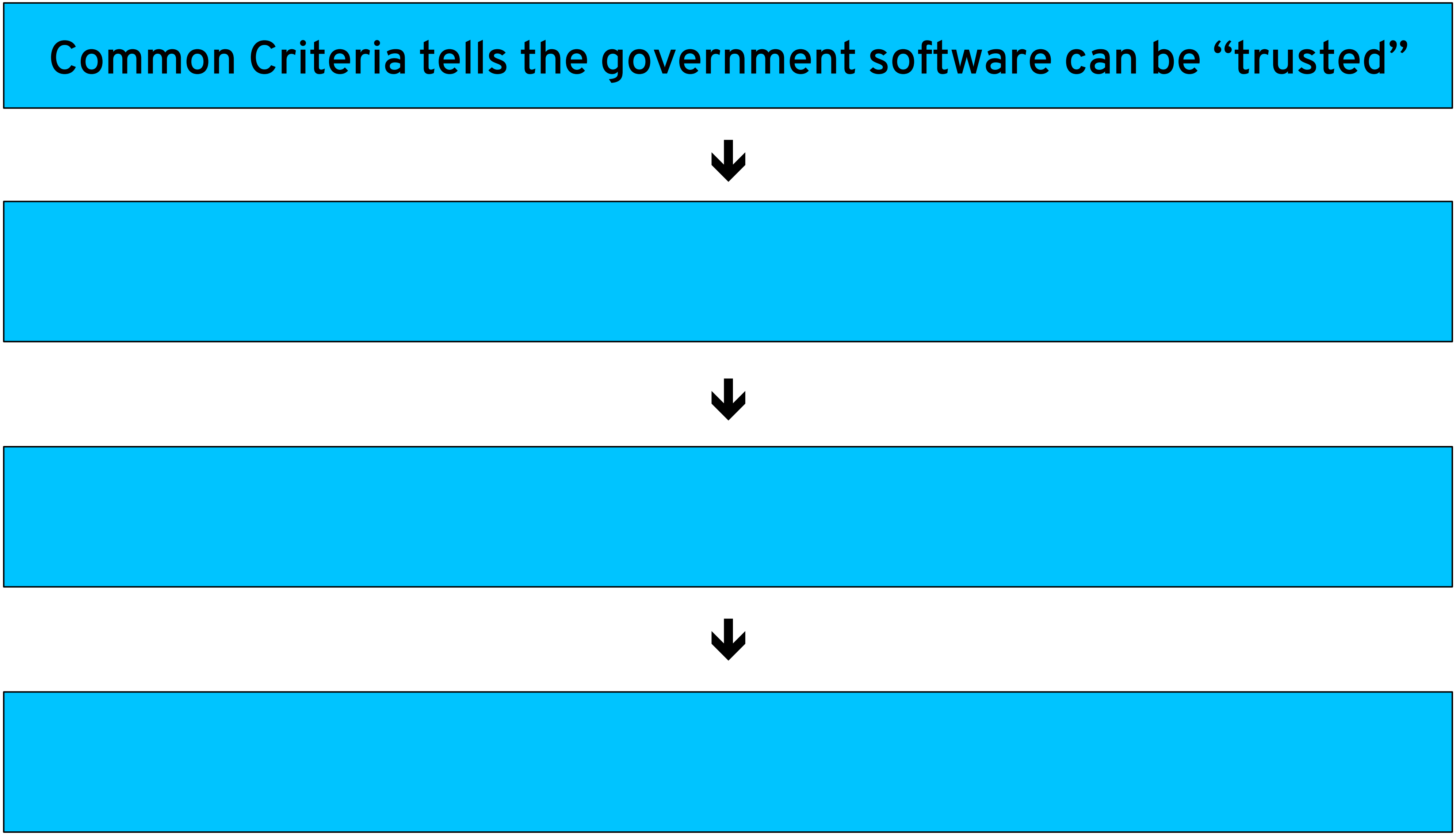
Average time to configure and verify control	# controls	Total time *per RHEL instance*
1 minute	* 587	9.7 hours
3 minutes	* 587	29.4 hours
5 minutes	* 587	48.9 hours

Common Criteria

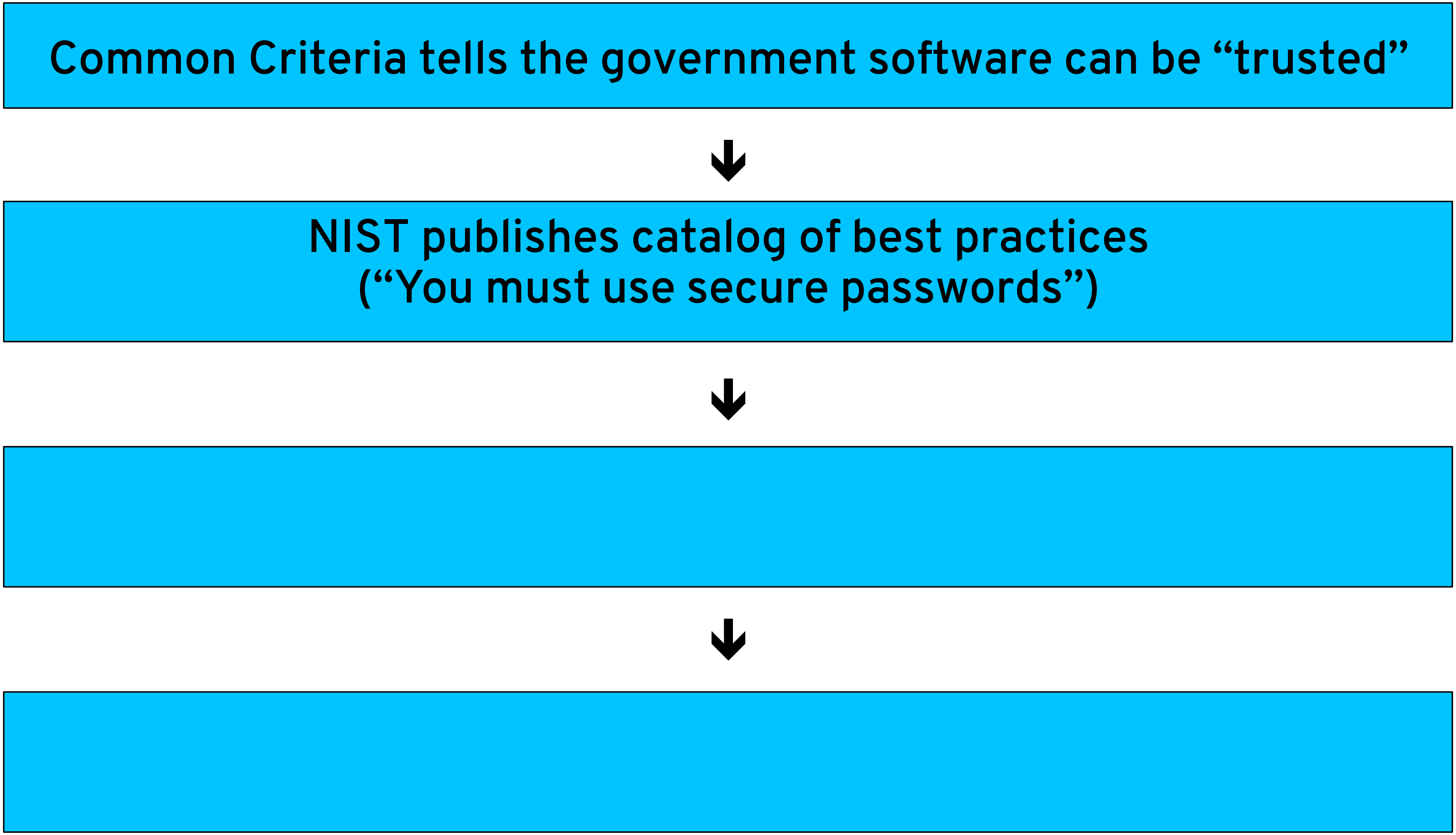
Common Criteria != Compliance Policy

	Red Hat Enterprise Linux 6 with KVM	Red Hat Enterprise Linux 5.6 with KVM	IBM z/VM Version 5 Release 3 (for IBM System z Mainframes)	VMWare vSphere 5.0	VMWare ESXi 4.1	Microsoft Windows Server 2008 Hyper-V Role with HotFix KB950050
Certification Date	2012-10-08	2012-04-20	2008-08-06	2012-05-18	2010-12-15	2009-07-24
EAL Level	EAP4+	EAP4+	EAP4+	EAP4+	EAP4+	EAP4+
CAPP	YES	YES	YES	NO	NO	NO
RBAC	YES	YES	NO	NO	NO	NO
LSPP	YES	YES	YES	NO	NO	NO

CAPP: Users control who access' their data
RBAC: Users classified into roles ("BackupAdm," "AuditAdm"...)
LSPP: Compartmentalizes users and applications from each other. Enables MLS.

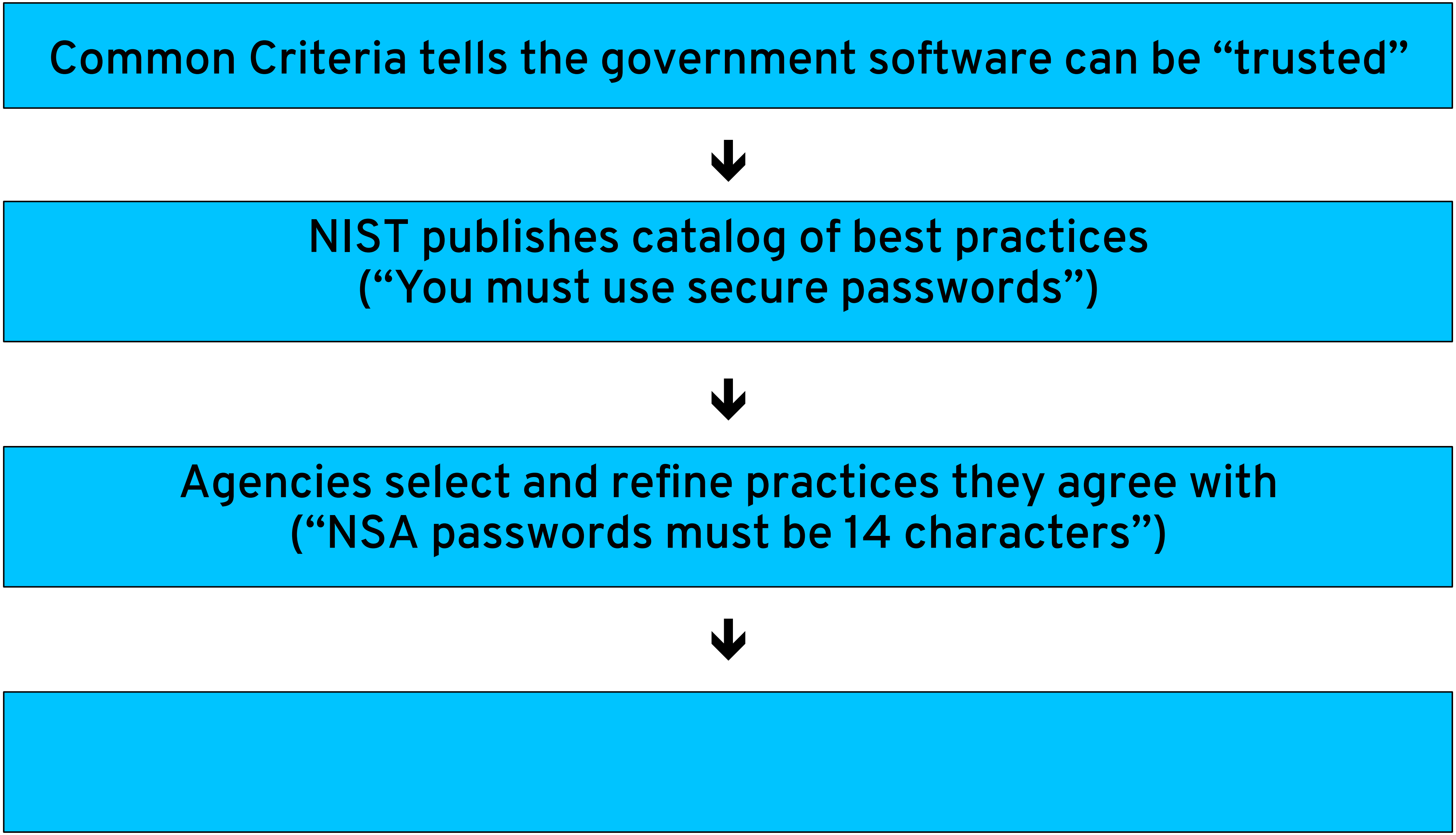


Common Criteria tells the government software can be “trusted”



Common Criteria tells the government software can be “trusted”

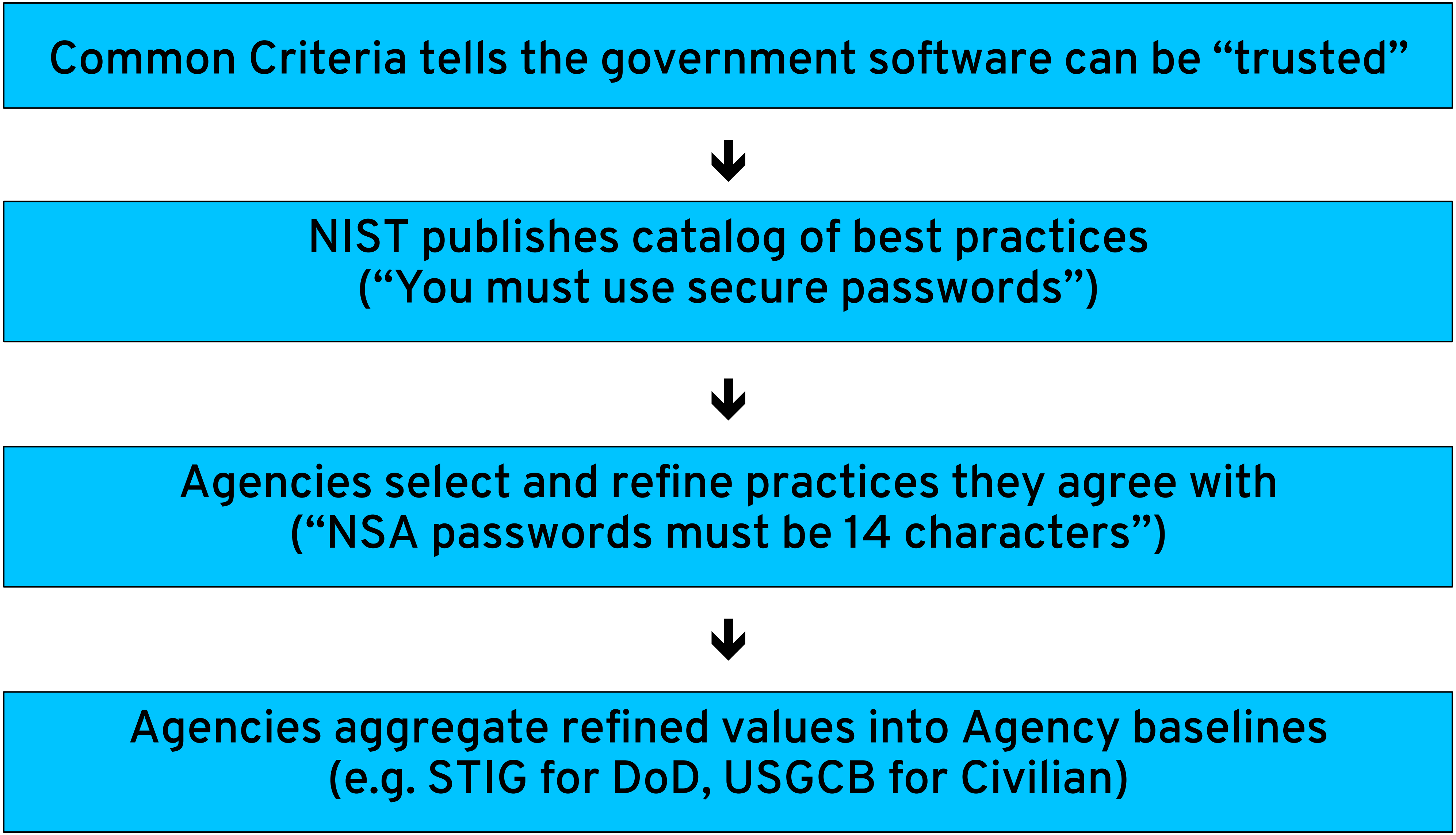
NIST publishes catalog of best practices
(“You must use secure passwords”)



Common Criteria tells the government software can be “trusted”

NIST publishes catalog of best practices
(“You must use secure passwords”)

Agencies select and refine practices they agree with
(“NSA passwords must be 14 characters”)



Common Criteria tells the government software can be “trusted”

NIST publishes catalog of best practices
(“You must use secure passwords”)

Agencies select and refine practices they agree with
(“NSA passwords must be 14 characters”)

Agencies aggregate refined values into Agency baselines
(e.g. STIG for DoD, USGCB for Civilian)

RHEL5 STIG Delay: 1,988 days

RHEL5 STIG Delay: 1,988 days

RHEL6 STIG Delay: 932 days

SCAP
Security Guide

DEFENSE INFORMATION SYSTEMS AGENCY

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

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

redhat

SCAP HTML

SCAP → HTML

OpenSCAP → Firefox

GUIDANCE

GUIDANCE	
VERIFICATION	

GUIDANCE	
VERIFICATION	
REMEDIATION	

GUIDANCE	XCCDF
VERIFICATION	
REMEDIATION	

GUIDANCE	XCCDF
VERIFICATION	OVAL
REMEDIATION	

GUIDANCE	XCCDF
VERIFICATION	OVAL
REMEDIATION	bash

I DON'T ALWAYS TEST MY CODE
BUT WHEN I DO,
IT'S DURING LIVE DEMOS

ROADMAP

- OpenStack Security Guide begins 24-JUNE-2013
  - Content will be incorporated into SCAP Security Guide
  - Formation of Red Hat OpenStack STIG (eta Q4 2013)
  - Want to participate? https://fedorahosted.org/scap-security-guide/
  - We need your feedback to prioritize other tech!
    - OpenShift vs JBoss vs Red Hat Storage vs ……..

MORE INFO

Web

http://fedorahosted.org/scap-security-guide

Mail

https://fedorahosted.org/mailman/listinfo/scap-security-guide

DISA STIG

http://iase.disa.mil/stigs/os/unix/red_hat.html

RED HAT SUMMIT

APPENDIX I:
Additional SSG Project Info

- Delivers practical security guidance, baselines, and associated validation mechanisms using the Security Content Automation Protocol (SCAP)
  - Current content for RHEL6, JBoss EAP5
- Upstream source for government *implementation* guidance
  - Specifically, DISA STIG and NSA SNAC Guide
  - First example of US Government policy, not just technology, derived from community open source project!

- Open Source project
  - https://fedorahosted.org/scap-security-guide
    (and yes, government can contribute!)
    (and yes, we checked with the lawyers)
- Why?
  - Enables agile government—vendor—consumer interaction
  - Ensures consensus among stakeholders
  - Enables development in SCAP formats

- Recommendations map to compliance standards wherever possible

- Because of this mapping, creation of custom "profiles" possible
  - RHEL6 STIG
  - RHEL6 Security Guide (via NSA)
  - Baseline content for FedRAMP
  - Your own?

- SCAP Formats
  - XML schemas, managed by NIST
  - Configuration checklist / guide format is XCCDF
  - Automated checking via OVAL

- COSTS
  - Complex XML schema
  - OVAL just a bit verbose </understatement>

- BENEFITS
  - Ingestible by SCAP-compatible tools
    - OpenSCAP ships within RHEL!
  - XCCDF Profiles
  - Standardized outputs/reporting

RED HAT SUMMIT

APPENDIX: USAGE DEMO

USE THE WORKBOOK!

- Available on wiki: https://fedorahosted.org/scap-security-guide/

STEP 1: DOWNLOAD

- RPM yum repository (EPEL)

```
$ sudo sh -c “wget -O /etc/yum.repos.d/epel-6-scap-security-guide.repo \
http://repos.fedorapeople.org/repos/scap-security-guide/epel-6-scap-security-
guide.repo”

$ sudo sh –c “yum install scap-security-guide”
```

- Source Code

```
$ git clone ssh://git.fedorahosted.org/git/scap-security-guide.git
```

- Note: RPMs place files into /usr/share/xml/scap/ssg

STEP 2: REVIEW GUIDANCE

- HTML guides located in /usr/share/xml/scap/ssg/guides/

- As of SSG v0.1-11, shipping EAP5 and RHEL6 guides

```
$ firefox \
/usr/share/xml/scap/ssg/guides/rhel6-guide.html
```

STEP 3: REVIEW POLICY MAPPINGS

- Policy mappings located in /usr/share/xml/scap/ssg/policytables/

- Frequently used as Security Requirements Traceability Matrix (STRM) foundations

```
$ firefox \
/usr/share/xml/scap/ssg/policytables/table-rhel6-
nistrefs.html
```

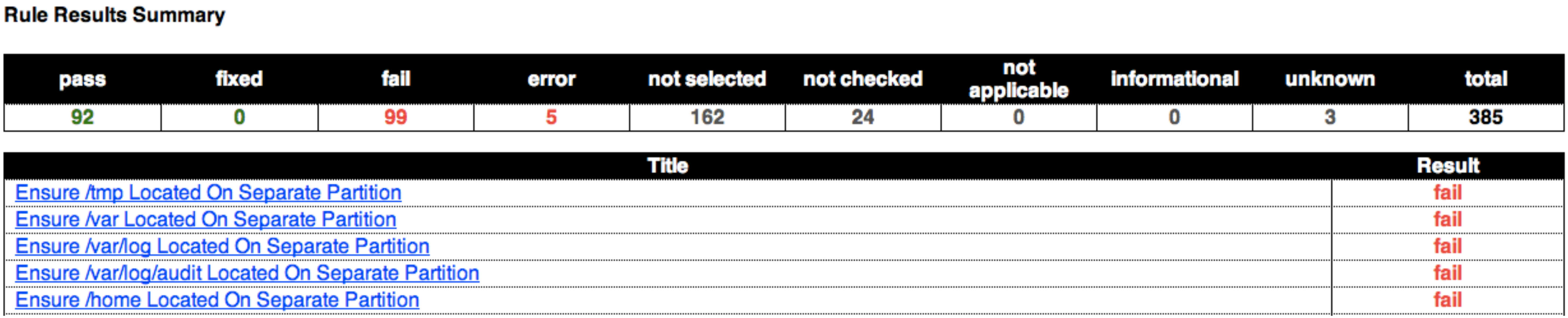
STEP 4: RUN A SCAN

```
$ sudo sh -c “oscap xccdf eval --profile stig-rhel6-server \
--results /root/ssg-results.xml \
--report /root/ssg-results.html \
--cpe /usr/share/xml/scap/ssg/content/ssg-rhel6-cpe-
dictionary.xml \
/usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml”
```

--results:	XML formatted results
--report:	HTML formatted results
Need help?	`man scap-security-guide`

STEP 5: REVIEW REPORT

```
$ firefox /root/ssg-results.html
```



Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
92	0	99	5	162	24	0	0	3	385

Title	Result
Ensure /tmp Located On Separate Partition	fail
Ensure /var Located On Separate Partition	fail
Ensure /var/log Located On Separate Partition	fail
Ensure /var/log/audit Located On Separate Partition	fail
Ensure /home Located On Separate Partition	fail

- Pass/fail “dashboard”
- Metadata of rules, once clicked

STEP 6: GENERATE REMEDIATION SCRIPTS

As of SSG v0.1-11 (e.g. June 2013)
this feature is undergoing rapid development. Not
complete, not fully tested, not ready for production!

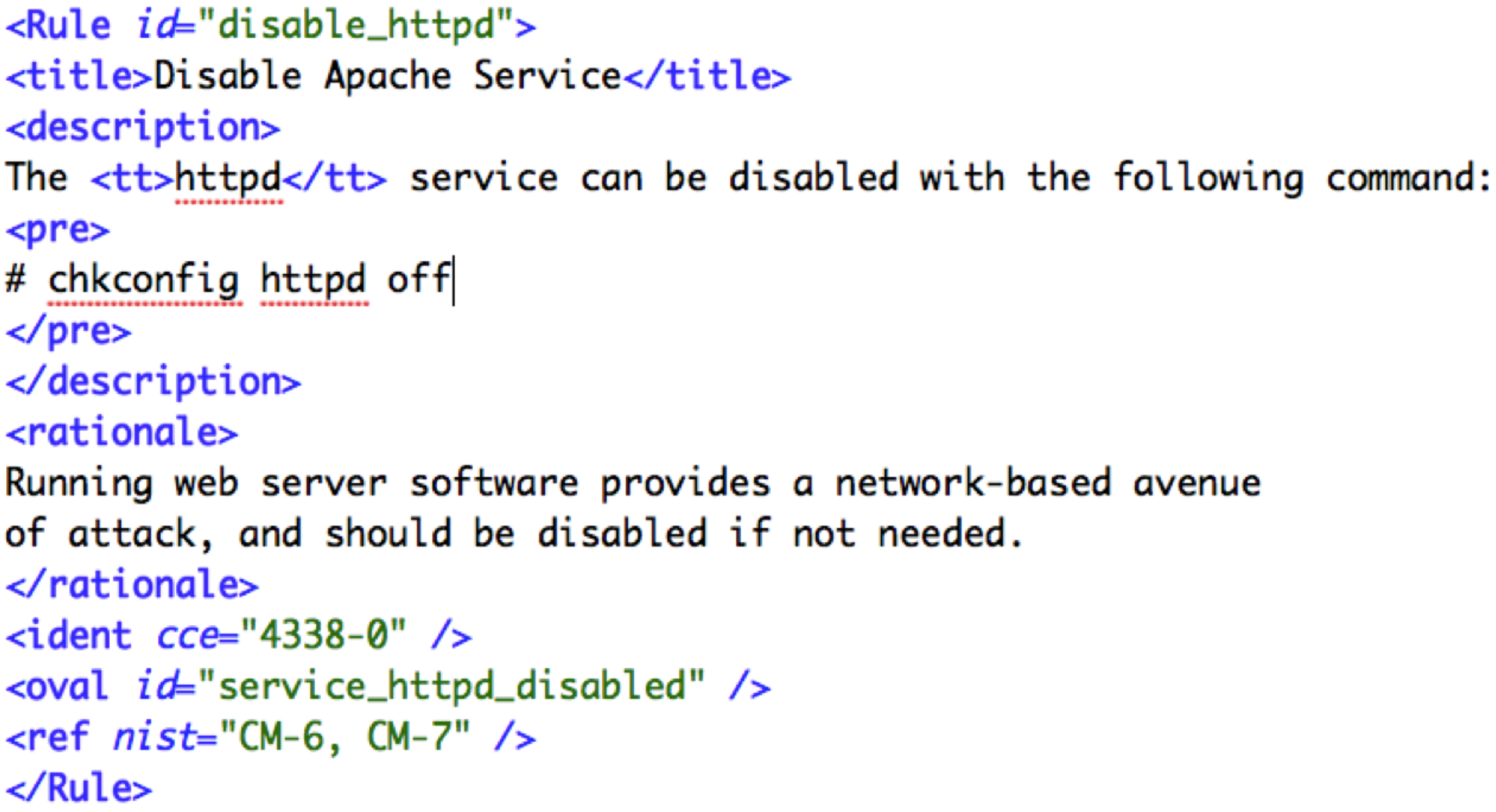
```
$ oscap xccdf generate fix \
--result-id xccdf_org.open-scap_testresult_stig-rhel6-server \
/var/www/html/results/results.xml
```

STEP 6: GENERATE REMEDIATION SCRIPTS

```
$ oscap xccdf generate fix \
--result-id xccdf_org.open-scap_testresult_stig-rhel6-server \
/var/www/html/results/results.xml
```

```
#!/bin/bash

# OpenSCAP fix generator output for benchmark: Guide to the
# Secure Configuration of Red Hat Enterprise Linux 6

# Generating fixes for all failed rules in test result
# 'xccdf_org.open-scap_testresult_stig-rhel6-server'.

# XCCDF rule: set_sysctl_net_ipv4_conf_all_accept_redirects
# CCE-27027-2
# Set runtime for net.ipv4.conf.all.accept_redirects

sysctl -q -n -w net.ipv4.conf.all.accept_redirects=0
if grep --silent ^net.ipv4.conf.all.accept_redirects /etc/sysctl.conf ; then
       sed –i \
            's/^net.ipv4.conf.all.accept_redirects.*/net.ipv4.conf.all.accept_redirects = 0/g' \
             /etc/sysctl.conf
else
       echo "" >> /etc/sysctl.conf
       echo "# Set net.ipv4.conf.all.accept_redirects to 0 per security requirements” \
            >> /etc/sysctl.conf
       echo "net.ipv4.conf.all.accept_redirects = 0" >> /etc/sysctl.conf
fi
```

STEP 7: XCCDF Review



```
<Rule id="disable_httpd">
<title>Disable Apache Service</title>
<description>
The <tt>httpd</tt> service can be disabled with the following command:
<pre>
# chkconfig httpd off
</pre>
</description>
<rationale>
Running web server software provides a network-based avenue
of attack, and should be disabled if not needed.
</rationale>
<ident cce="4338-0" />
<oval id="service_httpd_disabled" />
<ref nist="CM-6, CM-7" />
</Rule>
```

STEP 8: OVAL REVIEW

```
 <ind:textfilecontent54_object id="obj_20134" version="1">
    <ind:path>/etc</ind:path>
    <ind:filename>sysctl.conf</ind:filename>
    <ind:pattern operation="pattern match">^\s*net\.ipv6\.conf\.all
\.disable_ipv6\s*=\s*1$</ind:pattern>
    <ind:instance datatype="int">1</ind:instance>
  </ind:textfilecontent54_object>
```