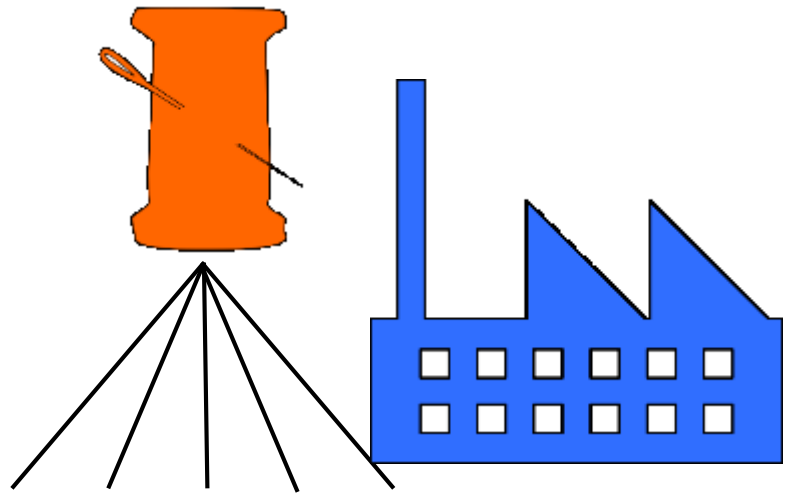
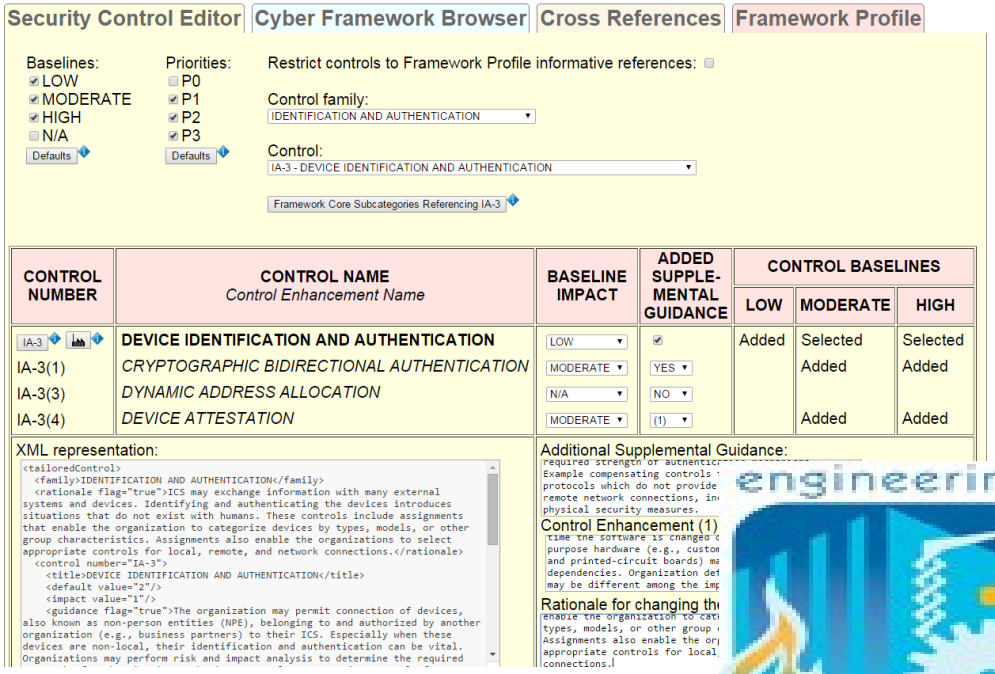
Baseline Tailor

Software-aided Security Control Selection

Joshua Lubell
Engineering Laboratory
April 21, 2016





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

engineering laboratory

Disclaimer

Certain commercial products are identified to help explain the research. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

Outline

- What, who, and why
- Baseline Tailor overview
- Demo: tailoring a security control
- Demo: supporting Risk Management Framework (RMF) **Select** step with a Cybersecurity Framework (CSF) Profile
- Concluding remarks

Examples inspired by guidance from NIST SP 800-82 (Guide to Industrial Control Systems Security)

What is Baseline Tailor?

Experimental open-source software for:

- Developing Cybersecurity Framework Profiles
- Tailoring National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls
- Generating Extensible Markup Language (XML) output
- Using the CSF and NIST SP 800-53 together

*Baseline Tailor supports the **Select** step of the RMF*

Potential Baseline Tailor Users

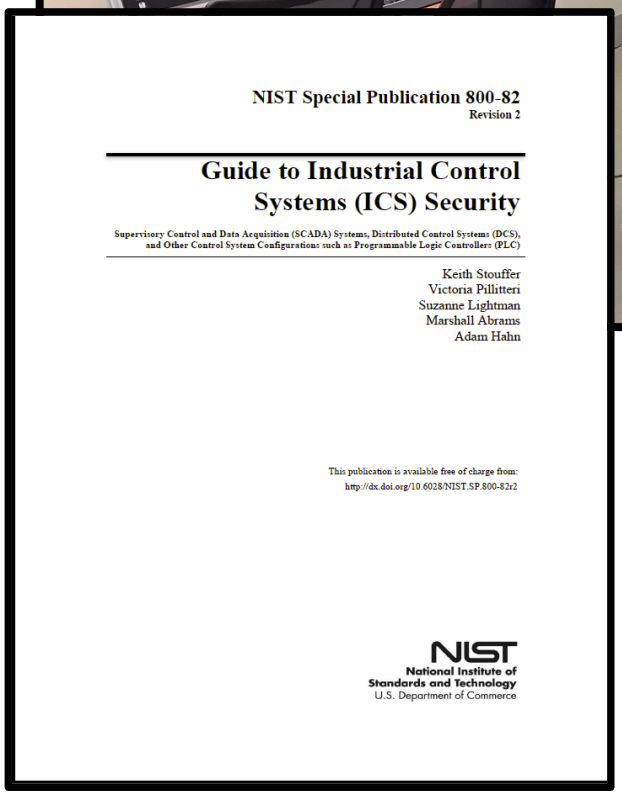
- People responsible for:
  - Information system development
  - Cybersecurity implementation and operation
- Developers of:
  - Industry sector-specific cybersecurity guidance
  - Cybersecurity-related software applications
- Organizations wishing to improve communication of cybersecurity information

Baseline Tailor Goals

- Make it easier to create and document Profiles, tailored baselines, overlays
- Enforce NIST SP 800-53 tailoring constraints
- Promote interoperability and reuse
- Enable security automation

About Me

- Relatively new to the world of cybersecurity
- Past experience with XML and data modeling
- Contributed to ISO 10303 (aka STEP) standard, used in most computer-aided design systems
- Member of NIST's **Cybersecurity for Smart Manufacturing Systems** project
  - Objective: Deliver a manufacturing-tailored cybersecurity RMF with supporting guidelines, methods, metrics and ***tools*** that addresses performance, reliability, and safety requirements



NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Victoria Pillitteri
Suzanne Lightman
Marshall Abrams
Adam Hahn

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

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

DRAFT

MANUFACTURING PROFILE

NIST Cybersecurity Framework

A Manufacturing-Sector tailored approach to protecting against cyber risk
April 2016

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

Mission 4 - Production Goals

ID.AM-1
ID.AM-2
ID.AM-3
ID.AM-4
ID.AM-5
ID.AM-6
ID.BE-1
ID.BE-2
ID.BE-3
ID.BE-4
ID.BE-5
ID.GV-1
ID.GV-2
ID.GV-3
ID.GV-4
ID.RA-1
ID.RA-2
ID.RA-3
ID.RA-4
ID.RA-5
ID.RA-6
ID.RM-1
ID.RM-2
ID.RM-3
PR.AC-1
PR.AC-2
PR.AC-3
PR.AC-4
PR.AC-5
PR.AT-1
PR.AT-2

Awareness and Training

Manufacturing Profile for Cyber Security Framework 12

Why I'm Here

- To get feedback
  - Is Baseline Tailor useful in its current state?
  - What would make it more useful?
  - Am I on the right track?

- To spread the word
  - Prospective users
  - Third-party developers (and those they listen to)

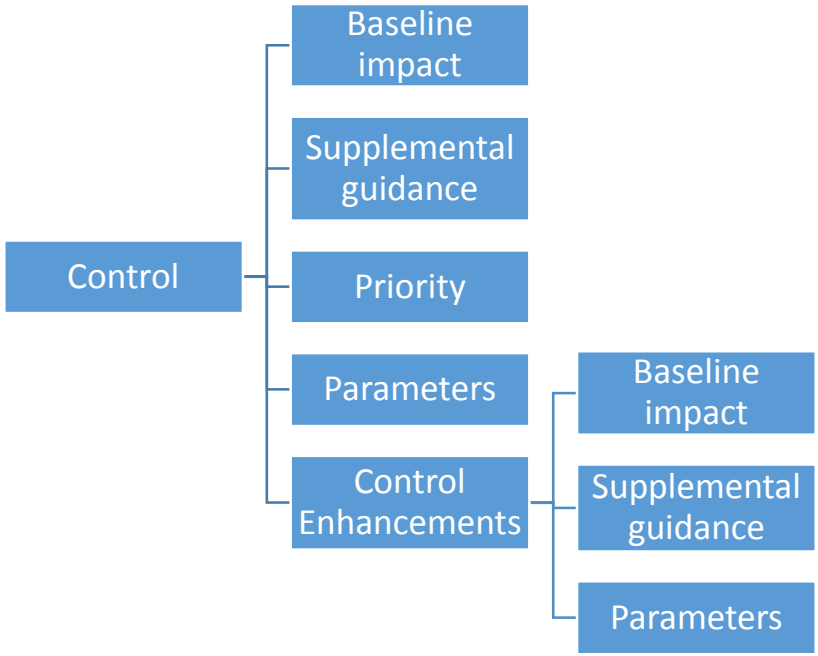
Why Baseline Tailor?

Reason 1: Incompatible representations

- NIST SP 800-82 Industrial Control System overlay documented as a series of tables
- Tailored baselines for mobile devices and cloud computing services each documented as spreadsheets
- All use divergent documentation conventions
- None are easy for users to navigate or for software developers to integrate

Reason 2: Challenges Combining RMF and CSF

Security Control

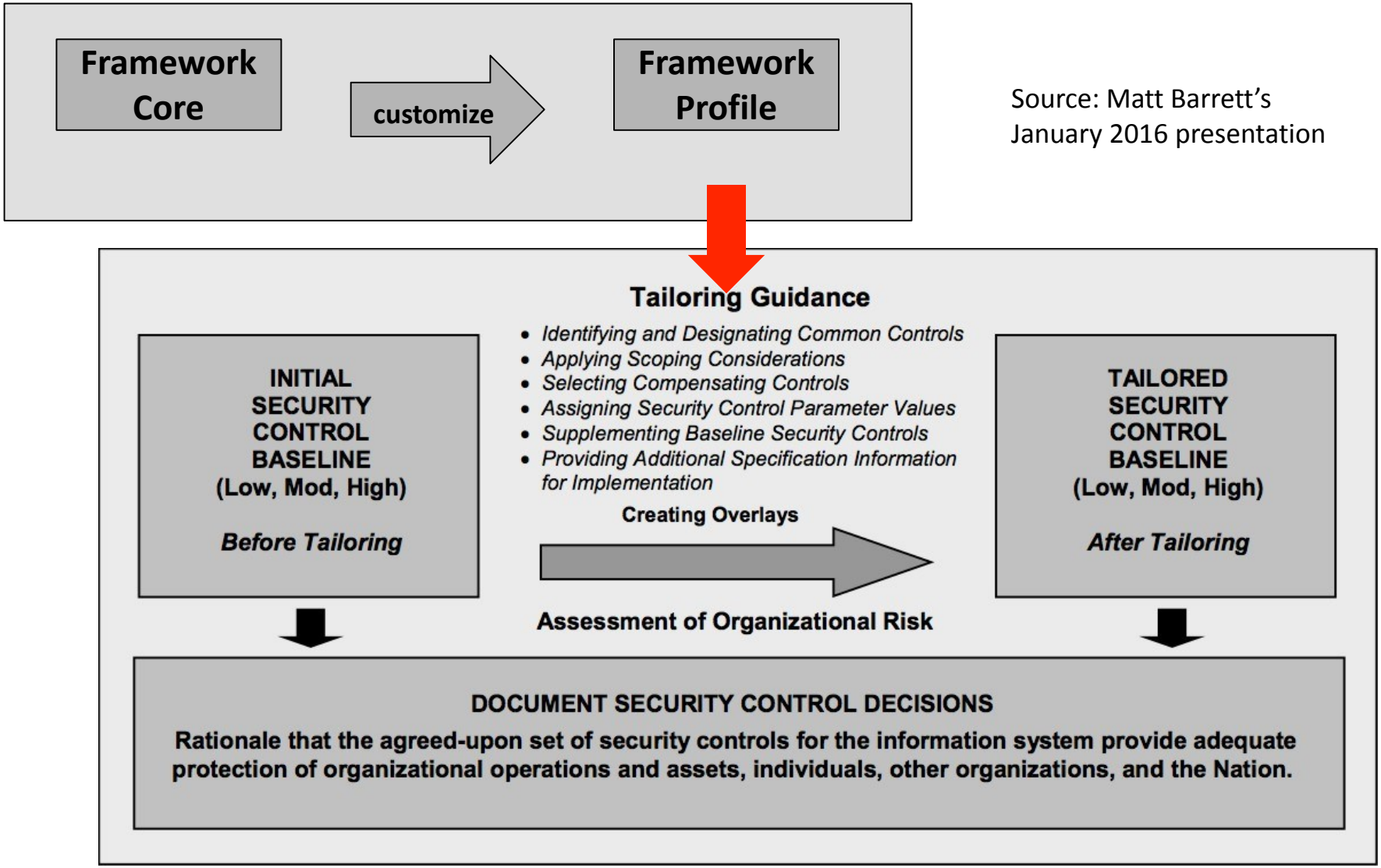


CSF Core

Functions	Categories	Subcategories	Informative References
Identify			
Protect			
Detect			
Respond			
Recover			

Tailoring SP 800-53 Security Controls

Use Case: Supporting the RMF Select step with a Framework Profile



Source: Matt Barrett's January 2016 presentation

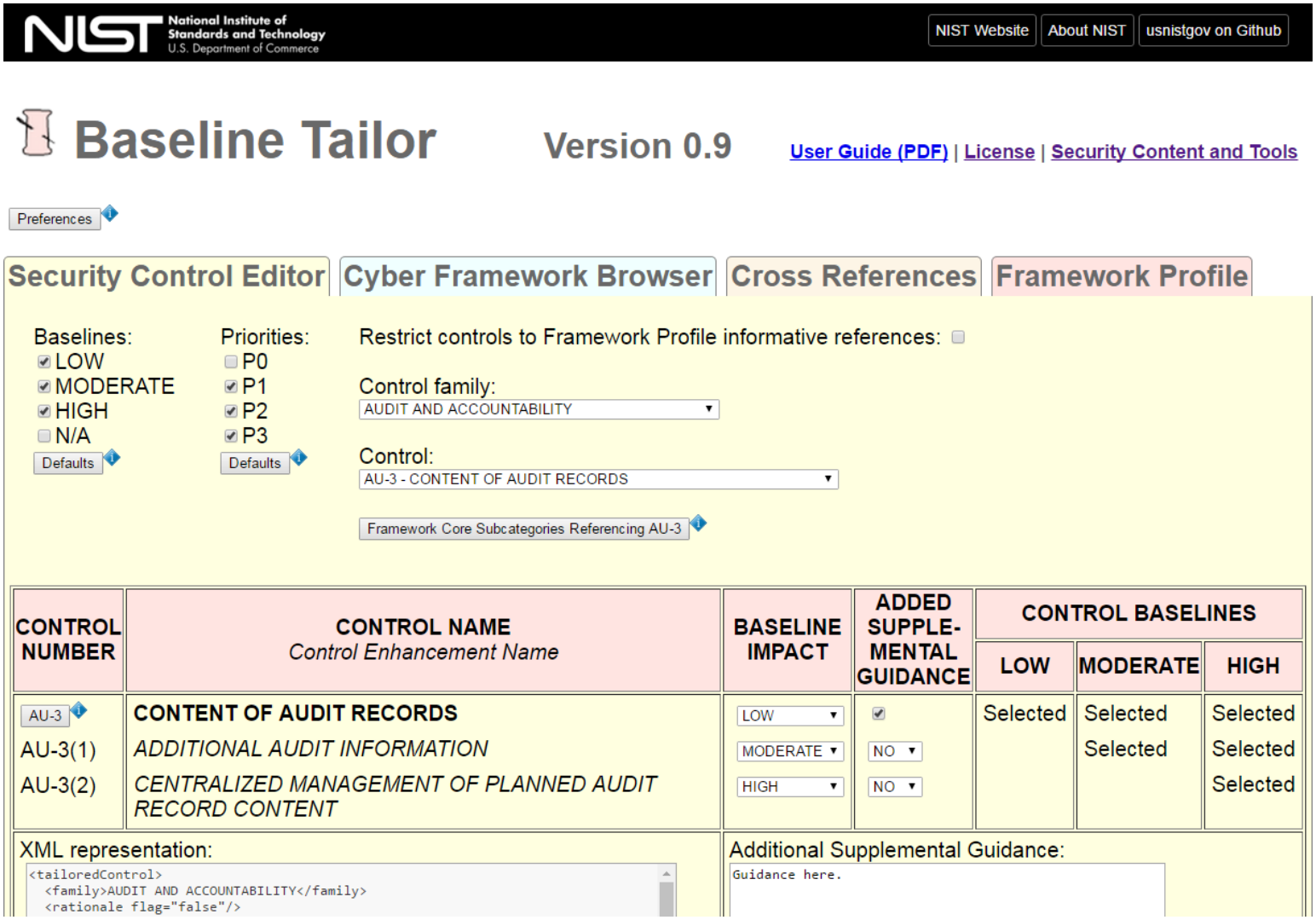
Outline

- What, who, and why
- Baseline Tailor overview
- Demo: tailoring a security control
- Demo: supporting the RMF Select step with a Framework Profile
- Concluding remarks

About Baseline Tailor

- Single-page web application
- Hosted at https://pages.nist.gov/sctools
- Easy to install and run locally
- Includes internal data model of CSF Core
- Leverages existing information sources
  - NIST SP 800-53 database (https://nvd.nist.gov/800-53)
    - XML NIST SP 800-53 Controls (Appendix F and G)
    - Online search
  - NIST SP 800-82 Industrial Control System baselines

Tabbed User Interface



What You Can Do With the Tabs

Tab	Operations
Security Control Editor	• Navigate security control catalog and ICS overlay • Modify baselines • Add to supplemental guidance
Cyber Framework Browser	• Navigate Core • Modify Profile
Cross References	• Show all Core subcategories referencing a control *Helpful for using CSF to support RMF **Select** step*
Framework Profile	• Modify Profile • View subcategory details

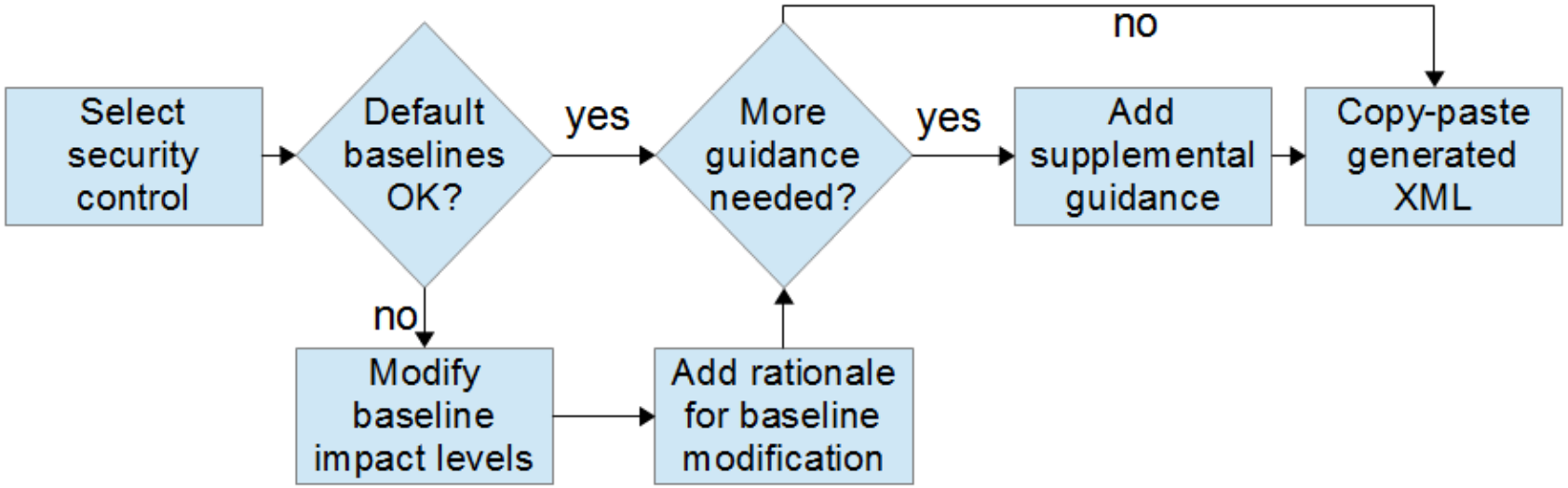
Baseline Tailor Implementation

- Source code is all XML (XForms, XSLT, XHTML)
  - Eases leveraging of NIST SP 800-53 XML data
  - Reduces dependence on programming/scripting languages
- All processing client side
- Runs in common browsers (Chrome, Firefox, Safari, Opera, …)
- Can be run from local file system without HTTP server

Outline

- What, who, and why
- Baseline Tailor overview
- Demo: tailoring a security control
- Demo: supporting the RMF Select step with a Framework Profile
- Concluding remarks

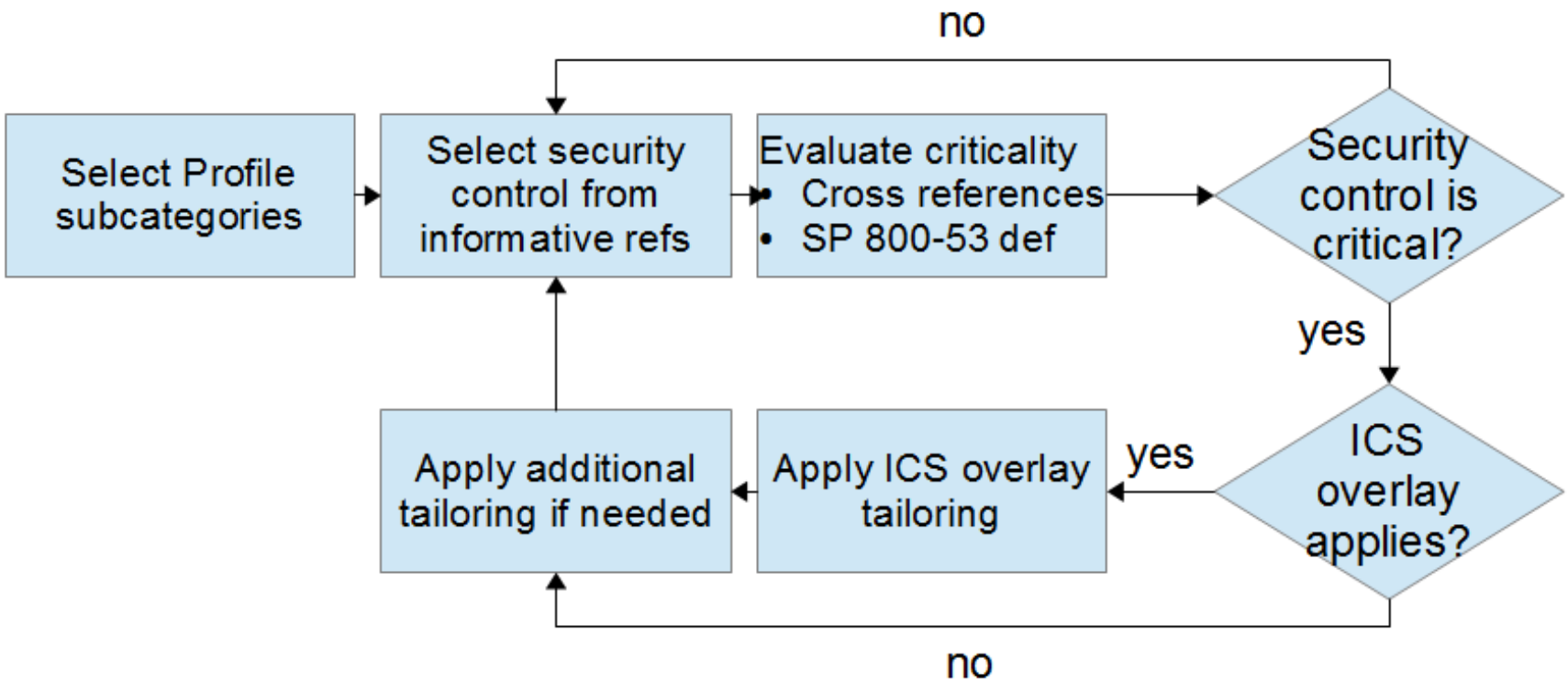
Security Control Editor Workflow



Outline

- What, who, and why
- Baseline Tailor overview
- Demo: tailoring a security control
- Demo: supporting the RMF **Select** step with a Framework Profile
- Concluding remarks

Workflow: Bringing it all Together



Outline

- What, who, and why
- Baseline Tailor overview
- Demo: tailoring a security control
- Demo: supporting the RMF Select step with a Framework Profile
- Concluding remarks

Summary

- Baseline Tailor is experimental open source software for CSF and NIST SP 800-53 RMF users
- Usage scenarios
  - Tailoring a security control
  - Browsing and using the CSF
  - Creating structured XML
  - Using the CSF and RMF together
  - *More likely to emerge*
- Was useful in creating CSF Manufacturing Profile employing NIST SP 800-53 and NIST SP 800-82 guidance

Limitations of Baseline Tailor

- Implementation tied to current versions on NIST specifications
  - New versions will require software updates
- Framework Profile XML could include more information
- Cannot import an existing tailored control
  - Needed for composability (e.g., tailoring an overlay)
- No support for NIST SP 800-53 assignment and selection parameters
  - Example from IA-3 description: "The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection."
- And many more…

A Plea

Security professionals:

- Try Baseline Tailor
- Encourage software developers to support CSF/RMF usage

Software developers:

- Experiment with the source code
- Build more and better tools

Everyone:

- Provide feedback, ask questions, report bugs

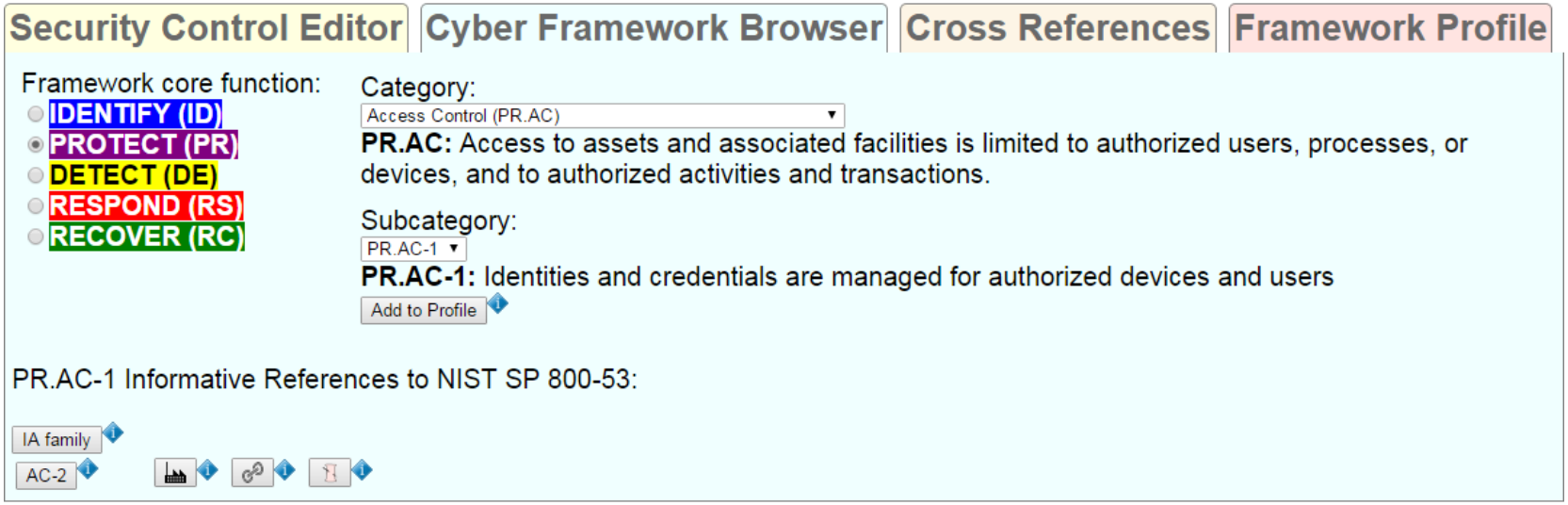
For More Information

- Baseline Tailor information page: http://go.usa.gov/cuxq3
- NIST Pages site: https://pages.nist.gov/sctools
  - Baseline Tailor online application
  - XML schemas and data
  - User Guide (NISTIR 8130)
- My email: lubell@nist.gov

Backup Slides

Preferences Dialog

Cyber Framework Browser Tab



Framework Profile Tab

Security Control Editor | Cyber Framework Browser | Cross References | Framework Profile

Check/uncheck the subcategory box to add to or remove the subcategory from the profile. Click the subcategory button to show its Framework Core information.

☐ ID.GV-1	☐ ID.RA-3	☑ PR.AC-1	☐ PR.IP-5	☐ PR.DS-4	☐ DE.CM-2	☐ DE.DP-1	☐ RS.CO-4
☐ ID.GV-2	☐ ID.RA-4	☑ PR.AC-2	☐ PR.IP-6	☐ PR.DS-5	☐ DE.CM-3	☐ DE.DP-2	☐ RS.CO-5
☐ ID.GV-3	☐ ID.RA-5	☑ PR.AC-3	☐ PR.IP-7	☐ PR.DS-6	☐ DE.CM-4	☐ DE.DP-3	☐ RS.MI-1
☐ ID.GV-4	☐ ID.RA-6	☑ PR.AC-4	☐ PR.IP-8	☐ PR.DS-7	☐ DE.CM-5	☐ DE.DP-4	☐ RS.MI-2
☐ ID.AM-1	☐ ID.BE-1	☑ PR.AC-5	☐ PR.IP-9	☐ PR.AT-1	☐ DE.CM-6	☐ DE.DP-5	☐ RS.MI-3
☐ ID.AM-2	☐ ID.BE-2	☐ PR.IP-1	☐ PR.PT-1	☐ PR.AT-2	☐ DE.CM-7	☐ RS.AN-1	☐ RS.RP-1
☐ ID.AM-3	☐ ID.BE-3	☐ PR.IP-10	☐ PR.PT-2	☐ PR.AT-3	☐ DE.CM-8	☐ RS.AN-2	☐ RS.IM-1
☐ ID.AM-4	☐ ID.BE-4	☐ PR.IP-11	☐ PR.PT-3	☐ PR.AT-4	☐ DE.AE-1	☐ RS.AN-3	☐ RS.IM-2
☐ ID.AM-5	☐ ID.BE-5	☐ PR.IP-12	☐ PR.PT-4	☐ PR.AT-5	☐ DE.AE-2	☐ RS.AN-4	☐ RC.RP-1
☐ ID.AM-6	☐ ID.RM-1	☐ PR.IP-2	☐ PR.DS-1	☐ PR.MA-1	☐ DE.AE-3	☐ RS.CO-1	☐ RC.CO-3
☐ ID.RA-1	☐ ID.RM-2	☐ PR.IP-3	☐ PR.DS-2	☐ PR.MA-2	☐ DE.AE-4	☐ RS.CO-2	☐ RC.IM-1
☐ ID.RA-2	☐ ID.RM-3	☐ PR.IP-4	☐ PR.DS-3	☐ DE.CM-1	☐ DE.AE-5	☐ RS.CO-3	☐ RC.IM-2

XML representation:

```
<frameworkProfile>
  <id>PR.AC-1</id>
  <id>PR.AC-2</id>
  <id>PR.AC-3</id>
  <id>PR.AC-4</id>
  <id>PR.AC-5</id>
</frameworkProfile>
```

Security Control Editor Tab: IA-3

Security Control Editor | Cyber Framework Browser | Cross References | Framework Profile

Baselines:
- [x] LOW
- [x] MODERATE
- [x] HIGH
- [ ] N/A

Defaults

Priorities:
- [ ] P0
- [x] P1
- [x] P2
- [x] P3

Defaults

Restrict controls to Framework Profile informative references: [ ]

Control family: IDENTIFICATION AND AUTHENTICATION

Control: IA-3 - DEVICE IDENTIFICATION AND AUTHENTICATION

Framework Core Subcategories Referencing IA-3

CONTROL NUMBER	CONTROL NAME *Control Enhancement Name*	BASELINE IMPACT	ADDED SUPPLE-MENTAL GUIDANCE	CONTROL BASELINES		
				LOW	MODERATE	HIGH
IA-3	**DEVICE IDENTIFICATION AND AUTHENTICATION**	MODERATE	[ ]		Selected	Selected
IA-3(1)	*CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*	N/A	NO			
IA-3(3)	*DYNAMIC ADDRESS ALLOCATION*	N/A	NO			
IA-3(4)	*DEVICE ATTESTATION*	N/A	NO			

NIST SP 800-53 Constraints

CONTROL NUMBER	CONTROL NAME *Control Enhancement Name*	BASELINE IMPACT	ADDED SUPPLE-MENTAL GUIDANCE	CONTROL BASELINES		
				LOW	MODERATE	HIGH
IA-3	**DEVICE IDENTIFICATION AND AUTHENTICATION**	MODERATE			Selected	Selected
IA-3(1)	*CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*	LOW	NO	Added	Added	Added
IA-3(3)	*DYNAMIC ADDRESS ALLOCATION*	N/A				
IA-3(4)	*DEVICE ATTESTATION*	N/A				

Control Enhancement impact lower than control impact.

CONTROL NUMBER	CONTROL NAME *Control Enhancement Name*	BASELINE IMPACT	ADDED SUPPLE-MENTAL GUIDANCE	CONTROL BASELINES		
				LOW	MODERATE	HIGH
IA-3	**DEVICE IDENTIFICATION AND AUTHENTICATION**	MODERATE			Selected	Selected
IA-3(1)	*CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*	MODERATE	YES		Added	Added
IA-3(3)	*DYNAMIC ADDRESS ALLOCATION*	N/A	NO			
IA-3(4)	*DEVICE ATTESTATION*	MODERATE	(3)		Added	Added

XML representation:

```
<tailoredControl>
  <family>IDENTIFICATION AND AUTHENTICATION</family>
  <rationale flag="true">Rationale here.</rationale>
  <control number="IA-3">
    <title>DEVICE IDENTIFICATION AND AUTHENTICATION</title>
    <default value="2"/>
```

Control Enhancement (

Guidance here.

Rationale for changing

ental Guidance:

Cross-reference to Control Enhancement without added supplemental guidance.

CONTROL NUMBER	CONTROL NAME *Control Enhancement Name*	BASELINE IMPACT	ADDED SUPPLE-MENTAL GUIDANCE	CONTROL BASELINES		
				LOW	MODERATE	HIGH
IA-3	**DEVICE IDENTIFICATION AND AUTHENTICATION**	MODERATE			Selected	Selected
IA-3(1)	*CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*	N/A	YES			
IA-3(3)	*DYNAMIC ADDRESS ALLOCATION*	N/A	NO			
IA-3(4)	*DEVICE ATTESTATION*	N/A	NO			

XML representation:

```
<tailoredControl>
  <family>IDENTIFICATION AND AUTHENTICATION</family>
  <rationale flag="false"/>
  <control number="IA-3">
```

Control Enhancement (

Guidance here.

ental Guidance:

Control Enhancement must have LOW, MODERATE, or HIGH impact if adding supplemental guidance.

IA-3 Tailored for an Industrial Control System

CONTROL NUMBER	CONTROL NAME *Control Enhancement Name*	BASELINE IMPACT	ADDED SUPPLE-MENTAL GUIDANCE	CONTROL BASELINES		
				LOW	MODERATE	HIGH
IA-3	**DEVICE IDENTIFICATION AND AUTHENTICATION**	LOW	☑	Added	Selected	Selected
IA-3(1)	*CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*	MODERATE	YES		Added	Added
IA-3(3)	*DYNAMIC ADDRESS ALLOCATION*	N/A	NO			
IA-3(4)	*DEVICE ATTESTATION*	MODERATE	(1)		Added	Added

XML representation:

```
<tailoredControl>
  <family>IDENTIFICATION AND AUTHENTICATION</family>
  <rationale flag="true">Rationale here.</rationale>
  <control number="IA-3">
    <title>DEVICE IDENTIFICATION AND AUTHENTICATION</title>
    <default value="2"/>
    <impact value="1"/>
    <guidance flag="true">Guidance here.</guidance>
  </control>
  <enhancement number="1">
    <title>CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION</title>
    <default value="4"/>
    <impact value="2"/>
    <guidance flag="true">Guidance here.</guidance>
  </enhancement>
  <enhancement number="4">
```

Additional Supplemental Guidance:

Guidance here.

Control Enhancement (1) Additional Supplemental Guidance:

Guidance here.

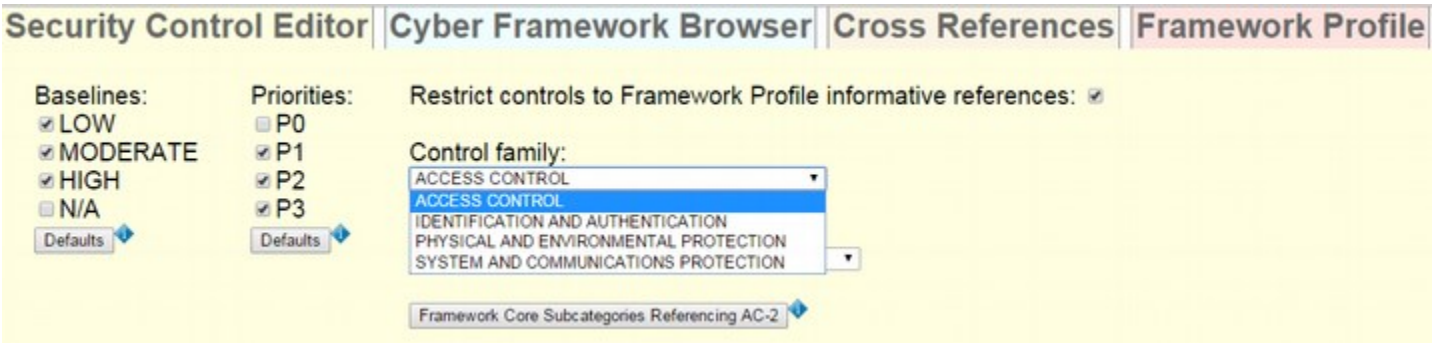
Rationale for changing the baseline:

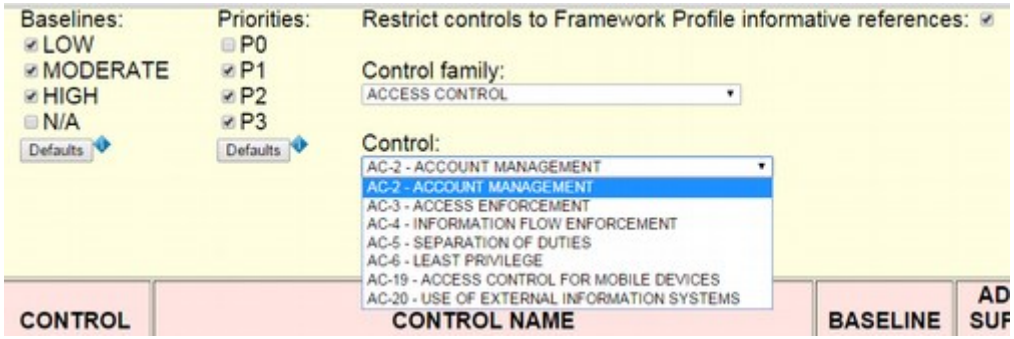
Rationale here.

ICS-specific Text Added, Copy-Pasted


```
<tailoredControl>
  <family>IDENTIFICATION AND AUTHENTICATION</family>
  <rationale flag="true">ICS may exchange information with many external systems and devices.
Identifying and authenticating the devices introduces situations that do not exist with
humans. These controls include assignments that enable the organization to categorize devices
by types, models, or other group characteristics. Assignments also enable the organizations
to select appropriate controls for local, remote, and network connections.</rationale>
  <control number="IA-3">
    <title>DEVICE IDENTIFICATION AND AUTHENTICATION</title>
    <default value="2"/><impact value="1"/>
    <guidance flag="true">The organization may permit connection of devices, also known as
non-person entities (NPE), belonging to and authorized by another organization (e.g.,
business partners) to their ICS. Especially when these devices are non-local, their
identification and authentication can be vital. Organizations may perform risk and impact
analysis to determine the required strength of authentication mechanisms. Example
compensating controls for devices and protocols which do not provide authentication for
remote network connections, include implementing physical security measures.</guidance>
  </control>
  <enhancement number="1">
    <title>CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION</title>
    <default value="4"/><impact value="2"/>
    <guidance flag="true">Configuration management for NPE identification and authentication
customarily involves a human surrogate or representative for the NPE. Devices are provided
with their identification and authentication credentials based on assertions by the human
surrogate. The human surrogate also responds to events and anomalies (e.g., credential
expiration). Credentials for software entities (e.g., autonomous processes not associated
with a specific person) based on properties of that software (e.g., digital signatures) may
change every time the software is changed or patched. Special purpose hardware (e.g., custom
integrated circuits and printed-circuit boards) may exhibit similar dependencies.
Organization definition of parameters may be different among the impact levels.</guidance>
  </enhancement>
  <enhancement number="4">
    <title>DEVICE ATTESTATION</title>
    <default value="4"/><impact value="2"/><guidance flag="1"/>
  </enhancement>
</tailoredControl>
```

Controls Referenced by PR.AC Subcategories





Security Control AC-2

CONTROL NUMBER	CONTROL NAME *Control Enhancement Name*	BASELINE IMPACT	ADDED SUPPLE-MENTAL GUIDANCE	CONTROL BASELINES		
				LOW	MODERATE	HIGH
AC-2	**ACCOUNT MANAGEMENT**	LOW		Selected	Selected	Selected
AC-2(1)	*AUTOMATED SYSTEM ACCOUNT MANAGEMENT*	MODERATE	NO		Selected	Selected
AC-2(2)	*REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*	MODERATE	NO		Selected	Selected
AC-2(3)	*DISABLE INACTIVE ACCOUNTS*	MODERATE	NO		Selected	Selected
AC-2(4)	*AUTOMATED AUDIT ACTIONS*	MODERATE	NO		Selected	Selected
AC-2(5)	*INACTIVITY LOGOUT*	HIGH	NO			Selected
AC-2(6)	*DYNAMIC PRIVILEGE MANAGEMENT*	N/A	NO			
AC-2(7)	*ROLE-BASED SCHEMES*	N/A	NO			
AC-2(8)	*DYNAMIC ACCOUNT CREATION*	N/A	NO			
AC-2(9)	*RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS*	N/A	NO			
AC-2(10)	*SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*	N/A	NO			
AC-2(11)	*USAGE CONDITIONS*	HIGH	NO			Selected
AC-2(12)	*ACCOUNT MONITORING / ATYPICAL USAGE*	HIGH	NO			Selected
AC-2(13)	*DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*	HIGH	NO			Selected

Cross References Tab

Security Control Editor | Cyber Framework Browser | Cross References | Framework Profile

Framework Core subcategories referencing control IA-3:

PR.AC-1

Security Control Editor | Cyber Framework Browser | Cross References | Framework Profile

Framework Core subcategories referencing control AC-2:

PR.AC-1

PR.AC-4

DE.CM-1

DE.CM-3

NIST SP 800-53 Database Lookup

AC-2 - ACCOUNT MANAGEMENT

Family: AC - ACCESS CONTROL

Priority: P1 - Implement P1 security controls first.

Baseline Allocation:

Low	Moderate	High
AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)

Jump To:
Revision 4 Statements
Control Description
Supplemental Guidance
References

Control Description

The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

g. Monitors the use of information system accounts;

h. Notifies account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;

j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and

k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

NIST SP 800-82 ICS

AC-2 ACCOUNT MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-2	**Account Management**	Selected	Selected	Selected
AC-2 (1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*		Selected	Selected
AC-2 (2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*		Selected	Selected
AC-2 (3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*		Selected	Selected
AC-2 (4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*		Selected	Selected
AC-2 (5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT / TYPICAL USAGE MONITORING*			Selected
AC-2 (11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*			Selected
AC-2 (12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*			Selected
AC-2 (13)	*ACCOUNT MANAGEMENT | ACCOUNT REVIEWS*			Selected

ICS Supplemental Guidance: Example compensating controls include providing increased physical security, personnel security, intrusion detection, auditing measures.
Control Enhancement: (1, 3, 4) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.
Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS (e.g., field devices) cannot support temporary or emergency accounts, this enhancement does not apply. Example compensating controls include employing nonautomated mechanisms or procedures.
Control Enhancement: (5) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.
Control Enhancement: (11, 12, 13) No ICS Supplemental Guidance.

Framework Core: Database Export


```
<RESULTSET FOUND="96">
  <ROW MODID="0" RECORDID="420">
    <COL>
      <DATA>IDENTIFY (ID)</DATA>
    </COL>
    <COL>
      <DATA>Governance (ID.GV): The policies, procedures, and processes to
manage and monitor the organization's regulatory, legal, risk, environmental,
and operational requirements are understood and inform the management of
cybersecurity risk.</DATA>
    </COL>
    <COL>
      <DATA>ID.GV-1: Organizational information security policy is
established</DATA>
    </COL>
    <COL>
      <DATA>·_____ NIST SP 800-53 Rev. 4 -1 controls from all families </DATA>
    </COL>
  </ROW>
  <ROW MODID="0" RECORDID="428">
    <COL>
      <DATA>IDENTIFY (ID)</DATA>
    </COL>
    <COL>
      <DATA>Governance (ID.GV): The policies, procedures, and processes to
manage and monitor the organization's regulatory, legal, risk, environmental,
and operational requirements are understood and inform the management of
cybersecurity risk.</DATA>
```

Structured XML via XSLT 2.0


```xml
<function id="ID">
   <name>IDENTIFY</name>
   <category id="ID.GV">
      <name>Governance</name>
      <dropDownLabel>Governance (ID.GV)</dropDownLabel>
      <description>The policies, procedures, and processes to manage and
monitor the organization's regulatory, legal, risk, environmental, and
operational requirements are understood and inform the management of
cybersecurity risk.</description>
      <subCategory id="ID.GV-1">
         <description>Organizational information security policy is
established</description>
         <sp800-53 all="true"/>
      </subCategory>
      <subCategory id="ID.GV-2">
         <description>Information security roles &amp; responsibilities are
coordinated and aligned with internal roles and external partners</description>
         <sp800-53>
            <control>PM-1</control>
            <control>PS-7</control>
         </sp800-53>
      </subCategory>
      <subCategory id="ID.GV-3">
         <description>Legal and regulatory requirements regarding
cybersecurity, including privacy and civil liberties obligations, are
understood and managed</description>
         <sp800-53 all="true">
            <except>PM-1</except>
```