Baseline Tailor
Software-aided Security Control Selection

Joshua Lubell
Engineering Laboratory
April 21, 2016
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
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

- Baseline impact
- Supplemental guidance
- Priority
- Parameters
- Control Enhancements

CSF Core

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respond</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recover</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Tailoring SP 800-53 Security Controls

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

Source: Matt Barrett’s January 2016 presentation

Tailoring Guidance
- Identifying and Designating Common Controls
- Applying Scoping Considerations
- Selecting Compensating Controls
- Assigning Security Control Parameter Values
- Supplementing Baseline Security Controls
- Providing Additional Specification Information for implementation

Creating Overlays

Assessment of Organizational Risk

DOCUMENT SECURITY CONTROL DECISIONS
Rationale that the agreed-upon set of security controls for the information system provide adequate protection of organizational operations and assets, individuals, other organizations, and the Nation.
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

Baseline Tailor

Version 0.9

Security Control Editor
- Baselines: LOW, MODERATE, HIGH, N/A
- Priorities: P0, P1, P2, P3

Cyber Framework Browser
- Restrict controls to Framework Profile informative references:
- Control family: AUDIT AND ACCOUNTABILITY
- Control: AU-3 - CONTENT OF AUDIT RECORDS
- Framework Core Subcategories Referencing AU-3:

<table>
<thead>
<tr>
<th>CONTROL NUMBER</th>
<th>CONTROL NAME</th>
<th>BASELINE IMPACT</th>
<th>ADDED SUPPLEMENTAL GUIDANCE</th>
<th>CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU-3</td>
<td>CONTENT OF AUDIT RECORDS</td>
<td>LOW, MODERATE, HIGH</td>
<td>NO, NO, NO</td>
<td>Selected, Selected, Selected</td>
</tr>
<tr>
<td>AU-3(1)</td>
<td>ADDITIONAL AUDIT INFORMATION</td>
<td>LOW, MODERATE, HIGH</td>
<td>NO, NO, NO</td>
<td>Selected, Selected, Selected</td>
</tr>
<tr>
<td>AU-3(2)</td>
<td>CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT</td>
<td>LOW, MODERATE, HIGH</td>
<td>NO, NO, NO</td>
<td>Selected, Selected, Selected</td>
</tr>
</tbody>
</table>

XML representation:
```xml
<tailoredControl>
  <family>AUDIT AND ACCOUNTABILITY</family>
  <rationale flag="false"/>
</tailoredControl>
```

Additional Supplemental Guidance:
Guidance here.
## What You Can Do With the Tabs

<table>
<thead>
<tr>
<th>Tab</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Control Editor</td>
<td>• Navigate security control catalog and ICS overlay</td>
</tr>
<tr>
<td></td>
<td>• Modify baselines</td>
</tr>
<tr>
<td></td>
<td>• Add to supplemental guidance</td>
</tr>
<tr>
<td>Cyber Framework Browser</td>
<td>• Navigate Core</td>
</tr>
<tr>
<td></td>
<td>• Modify Profile</td>
</tr>
<tr>
<td>Cross References</td>
<td>• Show all Core subcategories referencing a control</td>
</tr>
<tr>
<td></td>
<td><em>Helpful for using CSF to support RMF Select step</em></td>
</tr>
<tr>
<td>Framework Profile</td>
<td>• Modify Profile</td>
</tr>
<tr>
<td></td>
<td>• View subcategory details</td>
</tr>
</tbody>
</table>
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

1. Select security control
2. Default baselines OK?
   - Yes: More guidance needed?
     - Yes: Add supplemental guidance
     - No: Modify baseline impact levels
   - No: Add rationale for baseline modification
3. No: Copy-paste generated XML
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

1. Select Profile subcategories
2. Select security control from informative refs
3. Evaluate criticality
   - Cross references
     - SP 800-53 def
4. Security control is critical?
   - yes
     - ICS overlay applies?
     - yes
6. Apply ICS overlay tailoring
   - no
7. Apply additional tailoring if needed
   - no

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

Security Control Editor  Cyber Framework Browser  Cross Ref
Cyber Framework Browser Tab

Framework core function:
- IDENTIFY (ID)
- PROTECT (PR)
- DETECT (DE)
- RESPOND (RS)
- RECOVER (RC)

Category:
Access Control (PR.AC)
PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Subcategory:
- PR.AC-1
  PR.AC-1: Identities and credentials are managed for authorized devices and users

PR.AC-1 Informative References to NIST SP 800-53:
Framework Profile Tab

<table>
<thead>
<tr>
<th>Security Control Editor</th>
<th>Cyber Framework Browser</th>
<th>Cross References</th>
<th>Framework Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>CONTROL NUMBER</th>
<th>CONTROL NAME</th>
<th>BASELINE IMPACT</th>
<th>ADDED SUPPLEMENTAL GUIDANCE</th>
<th>CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>IA-3</td>
<td>DEVICE IDENTIFICATION AND AUTHENTICATION</td>
<td>MODERATE</td>
<td>N/A</td>
<td>Selected</td>
</tr>
<tr>
<td>IA-3(1)</td>
<td>CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION</td>
<td>MODERATE</td>
<td>N/A</td>
<td>Selected</td>
</tr>
<tr>
<td>IA-3(3)</td>
<td>DYNAMIC ADDRESS ALLOCATION</td>
<td>N/A</td>
<td>N/A</td>
<td>Selected</td>
</tr>
<tr>
<td>IA-3(4)</td>
<td>DEVICE ATTESTATION</td>
<td>N/A</td>
<td>N/A</td>
<td>Selected</td>
</tr>
</tbody>
</table>

- Baselines: LOW, MODERATE, HIGH, N/A
- Priorities: P0, P1, P2, P3

### Cyber Framework Browser
- Restrict controls to Framework Profile informative references:
- Control family: IDENTIFICATION AND AUTHENTICATION
- Control: IA-3 - DEVICE IDENTIFICATION AND AUTHENTICATION

### Framework Profile
- Framework Core Subcategories Referencing IA-3
NIST SP 800-53 Constraints

<table>
<thead>
<tr>
<th>CONTROL NUMBER</th>
<th>CONTROL NAME</th>
<th>BASELINE IMPACT</th>
<th>ADDED SUPPLEMENTAL GUIDANCE</th>
<th>CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>IA-3</td>
<td>DEVICE IDENTIFICATION AND AUTHENTICATION</td>
<td>MODERATE</td>
<td>Added</td>
<td>Selected</td>
</tr>
<tr>
<td>IA-3(1)</td>
<td>CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION</td>
<td>LOW</td>
<td>Added</td>
<td>Selected</td>
</tr>
<tr>
<td>IA-3(3)</td>
<td>DYNAMIC ADDRESS ALLOCATION</td>
<td>N/A</td>
<td>Added</td>
<td>Added</td>
</tr>
<tr>
<td>IA-3(4)</td>
<td>DEVICE ATTESTATION</td>
<td>N/A</td>
<td>Added</td>
<td>Added</td>
</tr>
</tbody>
</table>

XML representation:

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

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

Cross-reference to Control Enhancement without added supplemental guidance.
IA-3 Tailored for an Industrial Control System

<table>
<thead>
<tr>
<th>CONTROL NUMBER</th>
<th>CONTROL NAME</th>
<th>BASELINE IMPACT</th>
<th>ADDED SUPPLEMENTAL GUIDANCE</th>
<th>CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>IA-3</td>
<td>DEVICE IDENTIFICATION AND AUTHENTICATION</td>
<td>LOW</td>
<td>Added</td>
<td>Selected</td>
</tr>
<tr>
<td>IA-3(1)</td>
<td>CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION</td>
<td>MODERATE</td>
<td>Added</td>
<td>Added</td>
</tr>
<tr>
<td>IA-3(3)</td>
<td>DYNAMIC ADDRESS ALLOCATION</td>
<td>N/A</td>
<td>Added</td>
<td>Added</td>
</tr>
<tr>
<td>IA-3(4)</td>
<td>DEVICE ATTESTATION</td>
<td>MODERATE</td>
<td>Added</td>
<td>Added</td>
</tr>
</tbody>
</table>

XML representation:
```
<w:enhancement>
    <enhancement number="IA-3">  
        <title>DEVICE IDENTIFICATION AND AUTHENTICATION</title>  
        <value>1</value>  
        <control number="IA-3"/>
    </enhancement>
</w:enhancement>
```

Additional Supplemental Guidance:
```
Guidance here.
```

Rationale for changing the baseline:
```
Rationale here.
```
<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

<table>
<thead>
<tr>
<th>CONTROL NUMBER</th>
<th>CONTROL NAME</th>
<th>BASELINE IMPACT</th>
<th>CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-2(1)</td>
<td>AUTOMATED SYSTEM ACCOUNT MANAGEMENT</td>
<td>LOW&lt;br&gt;MODERATE&lt;br&gt;HIGH</td>
<td>Selected&lt;br&gt;Selected&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(2)</td>
<td>REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS</td>
<td>MODERATE&lt;br&gt;N/A&lt;br&gt;HIGH</td>
<td>Selected&lt;br&gt;Selected&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(3)</td>
<td>DISABLE INACTIVE ACCOUNTS</td>
<td>MODERATE&lt;br&gt;N/A&lt;br&gt;HIGH</td>
<td>Selected&lt;br&gt;Selected&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(4)</td>
<td>AUTOMATED AUDIT ACTIONS</td>
<td>MODERATE&lt;br&gt;N/A&lt;br&gt;HIGH</td>
<td>Selected&lt;br&gt;Selected&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(5)</td>
<td>INACTIVITY LOGOUT</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;N/A</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(6)</td>
<td>DYNAMIC PRIVILEGE MANAGEMENT</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;N/A</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(7)</td>
<td>ROLE-BASED SCHEMES</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;N/A</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(8)</td>
<td>DYNAMIC ACCOUNT CREATION</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;N/A</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(9)</td>
<td>RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;N/A</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(10)</td>
<td>SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;N/A</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(11)</td>
<td>USAGE CONDITIONS</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;N/A</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(12)</td>
<td>ACCOUNT MONITORING / ATYPICAL USAGE</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;N/A</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;Selected</td>
</tr>
<tr>
<td>AC-2(13)</td>
<td>DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;N/A</td>
<td>N/A&lt;br&gt;N/A&lt;br&gt;Selected</td>
</tr>
</tbody>
</table>
## Cross References Tab

<table>
<thead>
<tr>
<th>Security Control Editor</th>
<th>Cyber Framework Browser</th>
<th>Cross References</th>
<th>Framework Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Framework Core subcategories referencing control IA-3:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR.AC-1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Control Editor</th>
<th>Cyber Framework Browser</th>
<th>Cross References</th>
<th>Framework Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Framework Core subcategories referencing control AC-2:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR.AC-1</td>
<td>PR.AC-4</td>
<td>DE.CM-1</td>
<td>DE.CM-3</td>
</tr>
</tbody>
</table>
NIST SP 800-53 Database Lookup

**AC-2 - ACCOUNT MANAGEMENT**

<table>
<thead>
<tr>
<th>Family:</th>
<th>AC - ACCESS CONTROL</th>
<th>Priority:</th>
<th>P1 - Implement P1 security controls first.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td></td>
<td>Baseline Allocation:</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AC-2 (1) (2) (3) (4)</td>
</tr>
</tbody>
</table>

---

**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.
### AC-2 ACCOUNT MANAGEMENT

<table>
<thead>
<tr>
<th>CNTL NO.</th>
<th>CONTROL NAME</th>
<th>LOW</th>
<th>MOD</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-2</td>
<td>Account Management</td>
<td>Selected</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>AC-2 (1)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>AUTOMATED SYSTEM ACCOUNT MANAGEMENT</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>AC-2 (2)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>AC-2 (3)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>DISABLE INACTIVE ACCOUNTS</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>AC-2 (4)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>AUTOMATED AUDIT ACTIONS</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>AC-2 (5)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>INACTIVITY LOGOUT / TYPICAL USAGE MONITORING</td>
<td>Selected</td>
<td></td>
</tr>
<tr>
<td>AC-2 (11)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>USAGE CONDITIONS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2 (12)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>ACCOUNT MONITORING / ATYPICAL USAGE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2 (13)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>ACCOUNT REVIEWS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ICS Supplemental Guidance: Example compensating controls include providing increased physical security, personnel security, intrusion detection, and 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>
  </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>
    </COL>
  </ROW>
</RESULTSET>
<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 & 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>
      </sp800-53>
    </subCategory>
  </category>
</function>