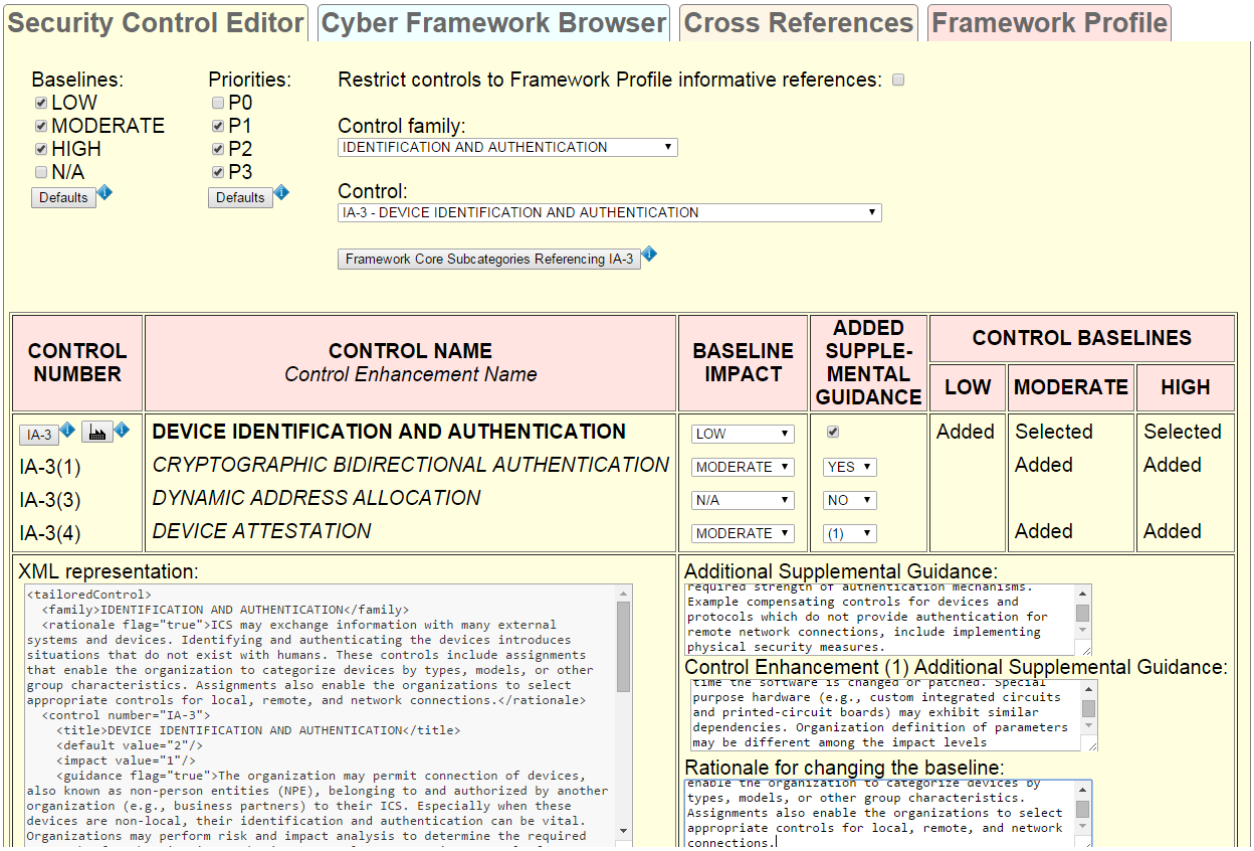
NISTIR 8130

Baseline Tailor User Guide

Joshua Lubell

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8130



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

NISTIR 8130

Baseline Tailor User Guide

Joshua Lubell
Systems Integration Division
Engineering Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8130

April 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Abstract

This guide describes how to use Baseline Tailor, a software tool for navigating the United States Government's Cybersecurity Framework and for tailoring the National Institute of Standards and Technology Special Publication 800-53 Revision 4 security controls. Baseline Tailor generates output in Extensible Markup Language (XML) formats capturing a user's Framework Profile and tailoring choices. More information about Baseline Tailor and supplemental documentation are available at http://www.nist.gov/el/msid/baselinetailor.cfm.

Disclaimers

Any mention of commercial or other third party products in this guide is for information purposes only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology (NIST). For any of the web links in the software and this user's guide, NIST does not necessarily endorse the views expressed, or concur with the facts presented on those web sites.

Baseline Tailor was developed at NIST by employees of the Federal Government in the course of their official duties. Pursuant to Title 17 Section 105 of the United States Code this software is not subject to copyright protection and is in the public domain. This software is an experimental system. NIST assumes no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Baseline Tailor uses XML data representing components defined in the NIST Framework for Improving Critical Infrastructure Cybersecurity and security controls and associated assessment procedures defined in NIST SP 800-53 Revision 4 Recommended Security Controls for Federal Information Systems and Organizations. For any discrepancies noted in the content between this XML data and the latest published NIST Cybersecurity Framework or Special Publication SP 800-53 Revision 4, please defer to the official published documents posted on http://csrc.nist.gov.

Baseline Tailor can be redistributed and/or modified freely provided that any derivative works bear some notice that they are derived from it, and any modified versions bear some notice that they have been modified. NIST would appreciate acknowledgement if the software is used.

Cover image: Security control IA-3 (Device Identification and Authentication) edited with Baseline Tailor, as per NIST Special Publication 800-82 overlay for Industrial Control Systems.

Acknowledgments

Baseline Tailor was developed as part of the Engineering Laboratory's Cybersecurity for Smart Manufacturing Systems project. I am grateful to my project colleagues, as well as colleagues from NIST's Computer Security Division and Applied Cybersecurity Division for their feedback, encouragement, and implementation suggestions. I also wish to thank Bob Lipman, KC Morris, and CheeYee Tang for their helpful reviews of earlier drafts of this document, and NIST's GitHub team for their support in deploying Baseline Tailor.

Table of Contents

List of Figures

1 Introduction

This guide describes how to use Baseline Tailor, a freely available and open source software tool, to aid in using the United States government's Cybersecurity Framework [1] and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 [2] security controls. Baseline Tailor usage scenarios include:

- Developing a Cybersecurity Framework Profile, covered in subsections 3.1 and 3.4.
- Tailoring security controls in accordance with NIST SP 800-53 guidelines, covered in subsection 3.2.
- Generating output in Extensible Markup Language (XML) [3] formats capturing a user's Framework Profile and tailoring choices, covered in subsections 3.2 and 3.4, and in section 5.
- Synthesizing into a coherent whole the security guidance from NIST SP 800-53, the Cybersecurity Framework, and related specifications, covered in section 4.

Potential users of Baseline Tailor, essentially the union of the NIST SP 800-53 and Cybersecurity Framework target audiences, include:

- People responsible for information system development.
- Organizations wishing to facilitate communication of cybersecurity information to stakeholders, including different levels of management.
- Developers of industry sector-specific cybersecurity guidance.
- People responsible for cybersecurity implementation and operation, such as business owners, owners of computers or cyber-physical systems, managers of digital repositories, system administrators, and information system security officers.
- Developers of cybersecurity-related software applications.

The primary goals of Baseline Tailor are to:

- Make it easier to create and document Framework Profiles, tailored baselines and overlays.
- Enforce constraints on tailoring operations to help ensure that the result follows NIST SP 800-53 guidelines.
- Generate XML valid with respect to schemas for Framework Profiles and tailored controls that can be used in conjunction with Framework Core XML data, NIST SP 800-53 XML data, and other XML-encoded security content to achieve security automation.

This guide assumes the reader is already familiar with the content of the following documents:

- The *Framework for Improving Critical Infrastructure Cybersecurity.* [1]
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* [2]

Both of these documents, as well as other information security standards, guidelines, and resources are available free of charge from NIST's Computer Security Resource Center (http://csrc.nist.gov).

The Cybersecurity Framework provides a way for organizations to describe their current security posture and target state, and to communicate and assess progress toward meeting goals. The heart of the Cybersecurity Framework is the Framework Core: a taxonomy of cybersecurity activities common across critical infrastructure sectors. The Framework Core is organized around specific outcomes, with each outcome containing references to standards addressing the outcome. A Framework Profile is a subset of the outcomes in the Framework Core representing either an organization's current or target security posture.

NIST SP 800-53 includes a catalog of tailorable security controls organized into eighteen families. Each control has zero or more control enhancements, each of which adds additional functionality to or increases the strength of the control. The catalog specifies three security control baselines: for low, moderate, and high impact information systems. NIST recommends the baselines as starting points for security control selection. For example, an organization looking to select security controls for a low impact system (where the consequences of compromised confidentiality, integrity, and availability of information are low) might begin with the controls in the baseline for the low impact level (or more succinctly, the low baseline) and tailor them as appropriate. In addition to baseline allocation, each security control is also assigned a priority code of P1, P2, P3, or P0. Controls with priority P1 should be implemented first, followed by those with priority P2, and finally those with priority P3. A P0 priority code indicates the security control is not assigned to a baseline.

NIST SP 800-53 also contains guidance for creating and documenting *overlays* to encourage the sharing of best security practices. An overlay is a set of control customizations applicable to a group of organizations with common security requirements. For example, NIST SP 800-82 (Guide to Industrial Control System Security) [4] specifies an overlay for Industrial Control Systems, which are common in the utility, transportation, chemical, pharmaceutical, process, and durable goods manufacturing industries. Industrial Control Systems are vulnerable to many of the same security threats that affect traditional information systems, yet have unique needs requiring additional guidance beyond that offered by NIST SP 800-53.

Baseline Tailor is a single-page web application. [5] Single-page applications, also known as AJAX (Asynchronous JavaScript [6] and XML) applications, run within a browser client such that the application's user interface state can update itself without server-side processing or page reloading. As a result, Baseline Tailor does not require a high speed Internet connection. Baseline Tailor can even be run offline without a Hypertext Transfer Protocol (HTTP) [7] server in browsers that that do not block read access to local files.

The Baseline Tailor user interface (discussed in section 3) provides context-sensitive search of the NIST SP 800-53 database, [8] an online version of the NIST SP 800-53 Revision 4 security control catalog, and also provides context-sensitive search of the NIST SP 800-82 overlay for Industrial Control Systems. The search capability enables the user to conveniently look up the

definition and guidance for the currently selected security control, or for security controls referenced by the current Framework Core selection.

Baseline Tailor adopts a minimalist approach. The software neither creates nor modifies any locally stored user files. Instead, Baseline Tailor displays its output in multiple-line, resizable text fields. The user can copy-paste this output into a third party XML editing application. Baseline Tailor's inability to directly write or modify files may seem limiting to some users. But other users may see this "limitation" as an advantage in that it allows for easy installation – even on systems with stringent security policies.

The remainder of this document is organized as follows:

- Section 2 discusses the requirements for running and, if necessary, installing Baseline Tailor.
- Section 3 documents Baseline Tailor's user interface by way of an extended example.
- Section 4 presents a scenario demonstrating how Baseline Tailor makes it easier to use the Framework Core, NIST SP 800-53 database and NIST SP 800-82 overlay together.
- Section 5 provides guidance on using the XML data that Baseline Tailor generates.
- Section 6 discusses some known issues and limitations, and provides other concluding remarks.

2 Getting Started

Baseline Tailor requires an Internet browser with support for JavaScript and the Extensible Stylesheet Language Transformations (XSLT) 1.0 standard. [9] Most of today's common browsers meet these requirements. Baseline Tailor has been successfully tested with recent versions of the Chrome, Firefox, Safari, and Opera browsers.[1]

Although not required, third party software for editing XML documents is desirable. A user can copy-paste Baseline Tailor's output into a plain text editor for further modification. However, software specifically designed for authoring XML data is easier to use, supports validation against a schema, and may also include other useful XML-specific functionalities.

Users may run Baseline Tailor online at https://pages.nist.gov/sctools/bt.xml. Baseline Tailor is also available as a zip file, downloadable from http://www.nist.gov/el/msid/baselinetailor.cfm, which users may install on an HTTP server or locally on their hard drive. To install, unzip the zip file. To run Baseline Tailor, open the file **`bt.xml`** in an Internet browser.

Users installing Baseline Tailor on their own HTTP server should make sure the server is configured to send files with **`.xml`** and **`.xsl`** suffixes as content type **`application/xml`**.

Users running Baseline Tailor from a local non-HTTP installation should follow instructions specific to their browser, if applicable, for allowing read access to files from the Baseline Tailor installation. For example, Chrome users running Baseline Tailor from a local non-HTTP

[1] For example, Baseline Tailor runs on a computer running Windows 7 in both Chrome version 49 and Firefox version 45.

installation should start up Chrome using the `--allow-file-access-from-files` command line option. Baseline Tailor runs locally in Firefox without any specialized browser configuration or startup options.

Baseline Tailor does not require a connection to the Internet to run. However, the NIST SP 800-53 database search function is unavailable without Internet access. As an offline workaround, users can instead refer to the security control catalog in Appendix F of a local copy of the NIST SP 800-53 Revision 4 document.

The source code for Baseline Tailor is publicly available at https://github.com/usnistgov/sctools.

3 User Interface

The Baseline Tailor user interface has four tabs:

- A Cyber Framework Browser tab for navigating the Framework Core and modifying a Framework Profile.
- A Security Control Editor tab for navigating the NIST SP 800-53 security control catalog and tailoring controls.
- A Framework Profile tab for modifying a Framework Profile and showing the currently-selected subset of Framework Core outcomes.
- A Cross References tab showing all references from the Framework Core to a particular security control.

A user may switch from one tab to another at any given time by clicking on the desired tab.

A user may click the "Preferences" button above the tabs, shown in Figure 1, to turn certain Baseline Tailor features on or off. Clicking the button causes the dialog shown in Figure 2 to appear. The "Security Control Editor tab" checkbox is selected by default. Unchecking this box hides the Security Control Editor tab, enabling a user not interested in tailoring security controls to reduce user interface clutter. The "NIST SP 800-82" checkbox, unchecked by default, turns on context-sensitive lookup of the NIST SP 800-82 Industrial Control Systems (ICS) overlay definitions. When done selecting preferences, the user clicks the "OK" button to hide the dialog.

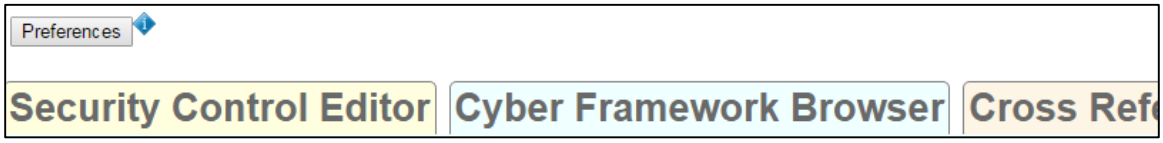


Figure 1. Preferences button above user interface tabs.

The following subsections describe the four Baseline Tailor user interface tabs in detail, using as an extended example the tailoring of security control IA-3 (Device Identification and Authentication) from the Identification and Authentication control family. IA-3 pertains to identifying and authenticating devices prior to connecting to them. In the example, IA-3 is tailored for Industrial Control Systems as specified in NIST SP 800-82. This example assumes that the user has selected both checkboxes in the preferences dialog.

Figure 2. Preferences dialog.

3.1 Cybersecurity Framework Browser

The Cyber Framework Browser tab supports the following operations:

- Navigating the Framework Core.
- Adding the subcategory being viewed to the Framework Profile.
- Removing a subcategory being viewed from the Framework Profile.

The Cyber Framework Browser tab includes the following user interface widgets:

- A set of radio buttons for choosing which of the five Framework Core functions to browse.
- A drop-down list of categories of outcomes associated with the selected function radio button.
- A drop-down list of subcategories representing specific outcomes associated with the currently selected category drop-down item.
- A button for adding the current subcategory selection to the Framework Profile or, if the subcategory selection is already in the Profile, removing the selected subcategory.
- For each security control referenced by the currently selected subcategory:
    - Buttons for NIST SP 800-53 database and NIST SP 800-82 ICS overlay lookup of the referenced security control.
    - A button for showing all Framework Core subcategories that reference the security control.
    - A button for tailoring the security control.

Figure 3 shows the Cyber Framework Browser tab after a user selects the radio button for the PROTECT (PR) Framework Core function. The "Category" drop-down list displays the category Access Control (PR.AC) – first in the list of categories associated with the PROTECT (PR) function. The user can select a different category by clicking on the drop-down arrow. The Framework Core description of the selected category appears below the drop-down list widget. The "Subcategory" drop-down list displays the subcategory PR.AC-1 – first in the list of subcategories associated with category PR.AC. The user can select a different subcategory by clicking on the drop-down arrow. The Framework Core description of the selected subcategory appears below the drop-down list widget.

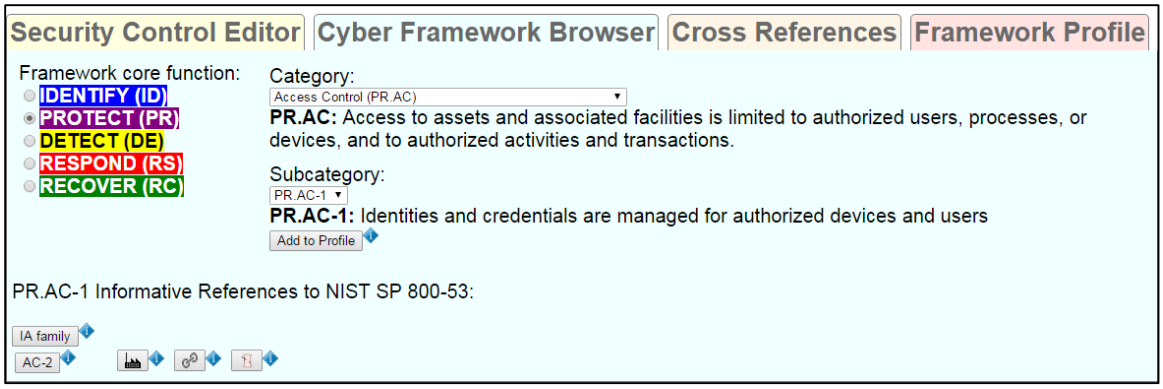


Figure 3. Cyber Framework Browser tab.

Below the description of subcategory PR.AC-1 is an "Add to profile" button the user can click on to add PR.AC-1 to the current Framework Profile. If PR.AC-1 had already been added, the button would instead say "Remove from Profile," and clicking would cause PR.AC-1 to be removed from the current Framework Profile. The current Framework Profile may also be modified using the widgets in the Framework Profile tab, discussed in subsection 3.4.

The bottom portion of Figure 3 contains buttons corresponding to NIST SP 800-53 security controls referenced by the subcategory PR.AC-1. These security controls include all controls belonging to the Identification and Authorization (IA) family, and security control AC-2 (Account Management) from the Access Control family. The user may click on the "IA family" or AC-2 buttons to search the NIST SP 800-53 online database in a new Internet browser tab.[2] Clicking the button with the factory image produces a new Internet browser tab with the ICS overlay definition for AC-2.[3] The user may view all the other Framework Core subcategories that reference AC-2 by clicking the button with the link image. Doing so causes the user interface to switch to the Cross References tab (described in subsection 3.3). The user may tailor security control AC-2 by clicking on the button with the needle-and-thread image.[4] Doing so causes the user interface to switch to the Security Control Editor tab (described in subsection 3.2).

3.2 Security Control Editor

The Security Control Editor tab supports the following operations:

- Navigating the NIST SP 800-53 security control catalog and NIST SP 800-82 overlay.
- Adding or removing controls or control enhancements to/from a baseline, and documenting the rationale for doing so as SP 800-53 requires.
- Adding additional supplemental guidance to a control or control enhancement in accordance with NIST SP 800-53 tailoring guidelines.

[2] By instructing the Internet browser to display the NIST SP 800-53 online database resource in a new tab, Baseline Tailor prevents loss of the current user interface state.
[3] This button appears only if the NIST SP 800-82 overlay box in the preferences dialog is checked.
[4] This button appears only if the Security Control Editor tab box in the preferences dialog is checked.

The Security Control Editor tab includes the following user interface widgets:

- Drop-down lists for choosing an individual control from a control family.
- Checkboxes and buttons for restricting the choices in the control drop-down list based on the NIST SP 800-53 baseline impact and priority.
- Buttons for showing the selected security control's cross references to Framework Core subcategories, and for NIST SP 800-53 database and NIST SP 800-82 overlay lookup.
- A table listing the selected security control and its control enhancements. The table includes widgets for modifying the baseline and for specifying whether the control or any control enhancements require additional supplemental guidance.
- Editable text fields for providing rationale and supplemental guidance. These text fields appear only if the user modifies the baseline or specifies that additional supplemental guidance is required.
- A non-editable text field showing an XML representation of the tailored security control.

The Security Control Editor is the most complex portion of Baseline Tailor's user interface. Figure 4 shows a high-level workflow of how one might use the Security Control Editor.[5] The user begins by choosing a security control to tailor. Next, if the user wishes to change the baseline impact for the security control or any of its control enhancements from the NIST SP 800-53 defaults, the user modifies the baseline impacts and provides text explaining the need for the changes. Then, if the user wishes to add supplemental guidance beyond the NIST SP 800-53 security control catalog supplemental guidance, the user provides the additional text. When done tailoring the security control, the user copy-pastes XML representing the tailored security control into third-party XML authoring software. The remainder of this subsection follows the Figure 4 workflow as applied to tailoring security control IA-3.

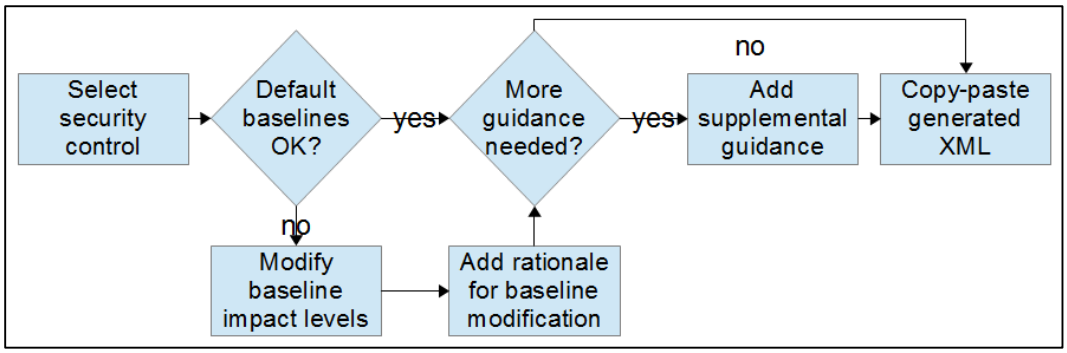


Figure 4. Security Control Editor workflow.

Figure 5 shows the upper portion of the Security Control Editor tab after the user has selected security control IA-3, but before initiating any tailoring. The two drop-down lists in the upper right hand corner are for choosing an individual control from a control family. The checkboxes and buttons to the left are for restricting the choices in the control drop-down list based on the NIST SP 800-53 baseline impact and priority. Checking the upper right checkbox restricts the

[5] This workflow is a suggestion only and does not preclude other possibilities.

control drop-down choices to those controls referenced by a subcategory in the current Framework Profile, shown in the Framework Profile tab (discussed in 3.4). By default, the control drop-down list contains all controls assigned to a NIST SP 800-53 baseline. Clicking on the "Framework Core subcategories referencing IA-3" button below the control drop-down list changes the focus to the Cross References tab (described in 3.4).

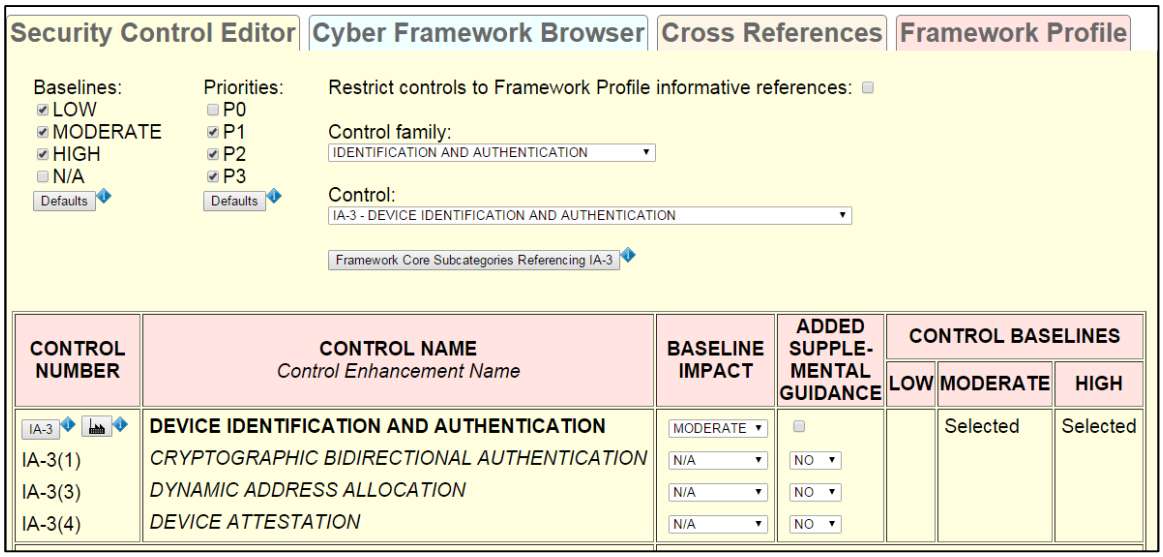


Figure 5. Security control IA-3.

The user's choice of IA-3 from the control drop-down list causes display of a table listing IA-3 with its control enhancements, as shown in the lower half of Figure 5. The two leftmost columns contain the identifier and name for the control and each of its enhancements. The control identifier appears as a button that the user can click to look up the control in the NIST SP 800-53 database. If the NIST SP 800-82 box in Preferences has been checked, a button with a factory image may be clicked to look up the control in the ICS overlay. The third column has drop-down lists for tailoring the baseline impact levels, each drop-down list offering the following choices:

- LOW: All baselines include the control or enhancement.
- MODERATE: The moderate and high baselines, but not the low baseline, include the control or enhancement.
- HIGH: Only the high baseline includes the control or enhancement.
- N/A: The control or enhancement is excluded from all baselines.

The values shown in Figure 5 are the defaults from the NIST SP 800-53 catalog, which includes IA-3 in the moderate and high baselines but not the low baseline[6], and excludes IA-3's enhancements from all three default baselines. The checkbox in the fourth column (ADDED SUPPLEMENTAL GUIDANCE) allows the user to provide additional supplemental guidance, beyond that given in NIST SP 800-53, for the control.

[6] IA-3 is not in the low baseline because NIST SP 800-53 assumes that low-impact systems are unlikely to have a need to connect directly to devices external to the organization.

The ADDED SUPPLEMENTAL GUIDANCE drop-down list for each enhancement allows the user to either

- Provide no additional supplemental guidance (NO),
- Provide additional supplemental guidance (YES), or
- Cross-reference supplemental guidance already added for another enhancement (cross-referenced enhancement number).

The three rightmost columns show the baseline selections for IA-3 and its enhancements. The selection text indicates the following:

- "Selected": The control or enhancement is in the NIST SP 800-53 baseline and has not been tailored out.
- "Added": The user has tailored in the control or enhancement.
- "Removed": The control or enhancement has been tailored out.
- Blank: The control or enhancement is not in the NIST SP 800-53 baseline and has not been tailored in.

The Security Control Editor displays appropriately worded alert messages if a user violates a tailoring constraint. For example, Figure 6 shows the result when attempting to add enhancement IA-3(1) to all baselines. This operation is illegal because it violates the constraint that an enhancement cannot be added to a baseline unless its parent control is added first. Thus, IA-3(1) cannot be added to the LOW baseline without first adding IA-3. Figure 7 shows the result when a control enhancement attempts to cross-reference another control enhancement, but the cross-referenced control enhancement lacks added supplemental guidance. Figure 8 shows the result when a user attempts to add supplemental guidance to a control enhancement before adding the control enhancement to a baseline.

Now suppose a user tailors IA-3 for Industrial Control Systems as per the NIST SP 800-82 ICS overlay. Since an ICS may need to connect directly to devices belonging to and authorized by third parties outside the organization, and these external devices need to be identified and authenticated, the user adds IA-3 to the low baseline. Additionally, the user adds control enhancements IA-3(1) and IA-3(4) to the moderate and high baselines in order to strengthen identification and authentication of external devices connected to by moderate and high-impact Industrial Control Systems. Finally, suppose the user wishes to add ICS-specific supplemental guidance applicable to IA-3 as a whole, as well as further ICS-specific supplemental guidance applicable to the control enhancements. To add the additional guidance, the user checks the box in the ADDED SUPPLEMENTAL GUIDANCE column, chooses YES from IA-3(1)' s ADDED SUPPLEMENTAL GUIDANCE drop-down list, and chooses (1) from IA-3(4)'s ADDED SUPPLEMENTAL GUIDANCE drop-down list.

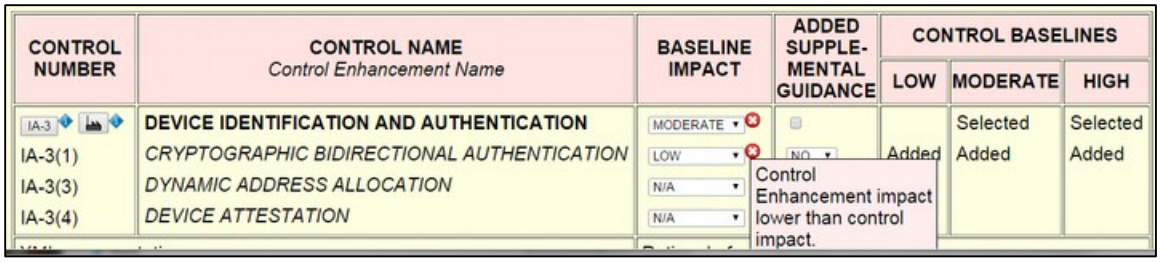


Figure 6. Violation of baseline impact constraint.

Figure 7. Violation of cross-reference constraint.

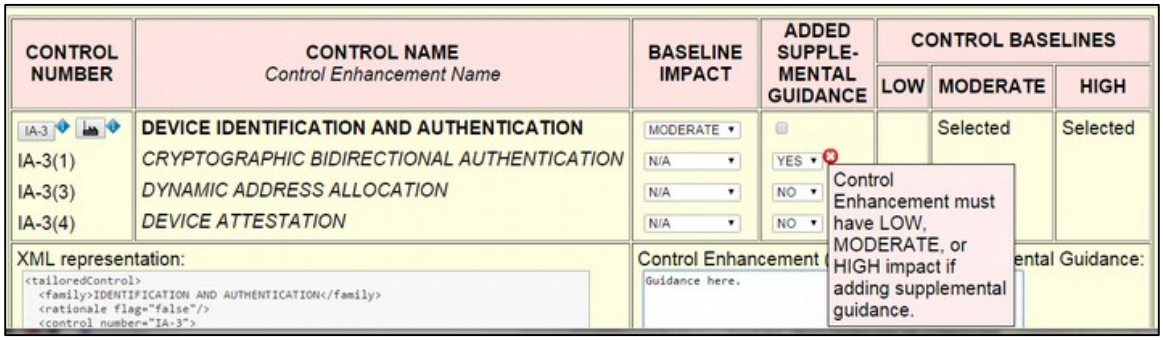


Figure 8. Violation of baseline constraint.

Figure 9 shows the result. Changing IA-3's baseline impact from MODERATE to LOW causes "Added" to appear in the LOW column. Changing the baseline impact for control enhancements IA-3(1) and IA-3(4) from N/A to MODERATE causes "Added" to appear in the MODERATE and HIGH control baseline columns. The baseline changes generate a "Rationale for changing the baseline" editable text field on the lower right for providing a rationale. Checking the box in the ADDED SUPPLEMENTAL GUIDANCE column generates an "Additional Supplemental Guidance" editable text field for adding the ICS-specific guidance applicable to IA-3 as a whole. Choosing YES from IA-3(1)' s ADDED SUPPLEMENTAL GUIDANCE drop-down list generates a "Control Enhancement (1) Additional Supplemental Guidance" editable text field for adding IA-3(1) supplemental guidance. Cross-referencing IA-3(1)'s added supplemental guidance from IA-(4) does not trigger an alert because IA-3(1)'s drop-down is set to YES.

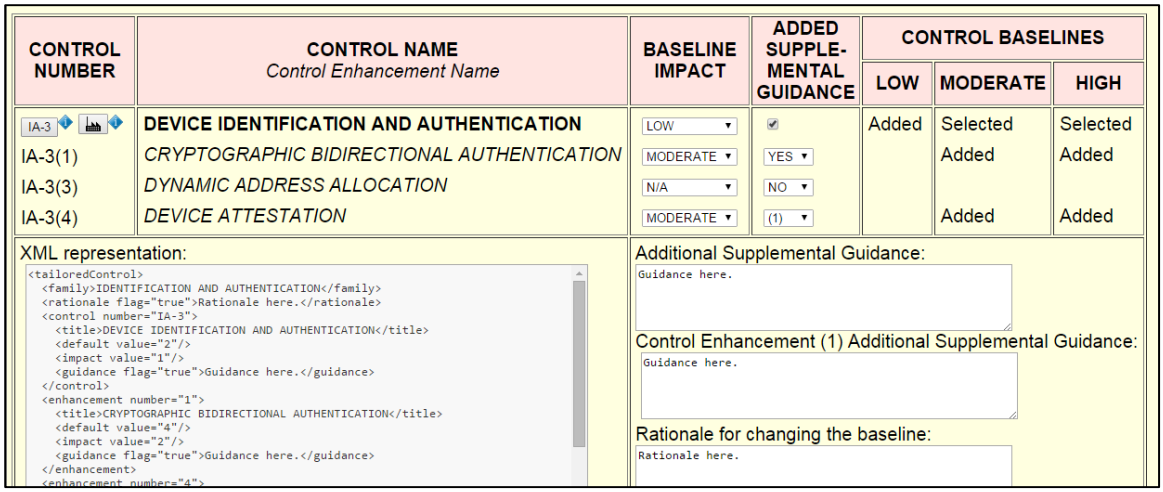


Figure 9. IA-3 tailored for an Industrial Control System.

The non-editable "XML representation" text field on the lower left shows XML generated on the fly based on the drop-down and checkbox settings and editable text field contents. Modifying the editable text fields on the right causes the contents of the "XML representation" text field to update in real time. In Figure 9, the editable text fields contain stub text. Figure 10 shows the text fields after adding supplemental guidance for IA-3 and IA-3(1), and providing a rationale for changing the IA-3 baseline. Notice that the "XML representation" content now includes the added guidance text. Section 5 provides additional details on the XML formats Baseline Tailor generates.

Now suppose the user is authoring a tailored baseline or overlay in a third-party XML application. At this point, the user would typically copy-paste the "XML representation" text into an XML authoring application. Figure 11 shows how the copy-pasted result might look. The Baseline Tailor distribution includes XML schemas (discussed in section 5) for use with third-party XML authoring tools.

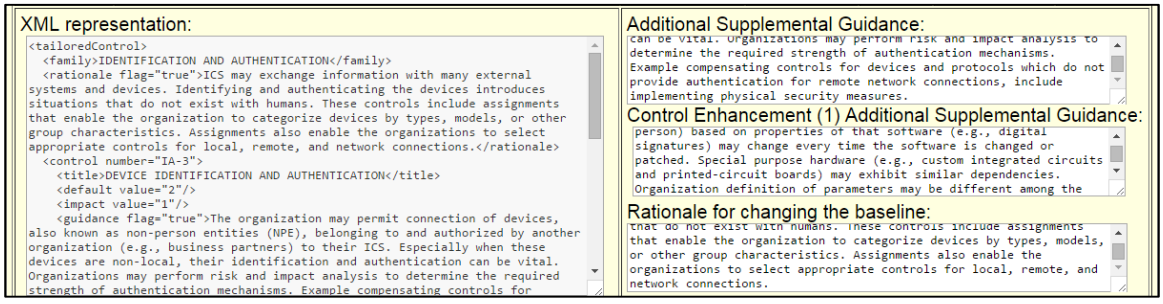


Figure 10. IA-3 text fields with ICS-specific guidance replacing stubs.

```
<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>
```

Figure 11. XML generated by the Security Control Editor copy-pasted into a third party XML authoring software application.

3.3 Cross References

The Cross References tab supports just one operation:

- Showing all Framework Core subcategories referencing a security control.

The Cross References tab includes the following user interface widgets:

- Buttons representing the cross referenced subcategories, any of which may be clicked to display the subcategory in the Cyber Framework Browser tab.

The Baseline Tailor user interface provides two ways a user can specify the security control whose cross references are displayed. The first way, discussed in subsection 3.1, is by clicking a button in the Cyber Framework Browser tab with a link image. The second way, discussed in subsection 3.2, is by clicking on the "Framework Core subcategories referencing…" button in

the Security Control Editor tab. Performing either action changes the focus to the Cross References tab.

Suppose the Security Control Editor tab appears as shown in Figure 5, and the user has clicked the "Framework Core subcategories referencing IA-3" button. Then the Cross References tab would appear as shown in Figure 12. As the figure shows, PR.AC-1 is the only subcategory referencing IA-3. Clicking the PR.AC-1 button causes the focus to change to the Cyber Framework Browser tab, with PROTECT (PR) selected from the "Framework core function" radio buttons, PR.AC selected from the "Category" drop-down list, and "PR.AC-1" selected from the "Subcategory" drop-down list.

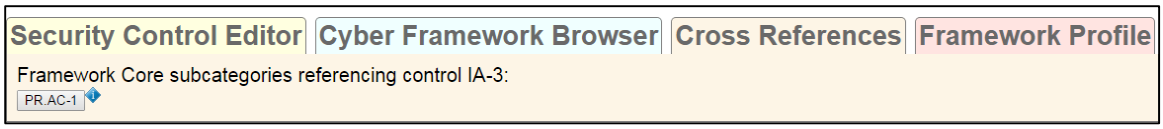


Figure 12. Subcategory referencing IA-3.

Figure 13 shows the Cross References tab when the Security Control Editor selection is AC-2 (Account Management) from the Access Control family, and the user has clicked the "Framework Core subcategories referencing AC-2" button. As Figure 13 shows, four Framework Core subcategories reference AC-2. Clicking any of these subcategory buttons causes a focus change to the Cyber Framework Browser tab, with the appropriate widget selections.

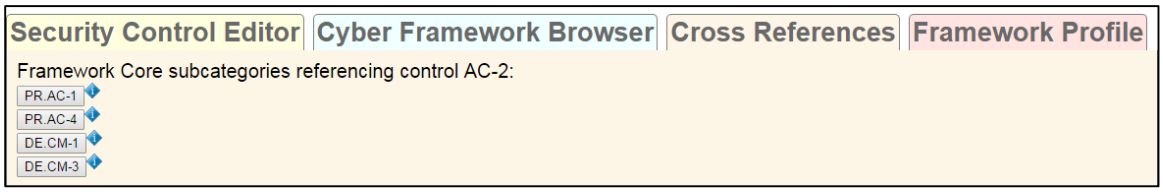


Figure 13. Subcategories referencing AC-2.

3.4 Framework Profile

The Framework Profile tab supports the following operations:

- Adding subcategories to the Framework Profile.
- Removing subcategories from the Framework Profile.
- Viewing a subcategory's description in the Cyber Framework Browser tab.

The Framework Profile tab includes the following user interface widgets:

- For each of the ninety-six Framework Core subcategories with informative references to NIST SP 800-53, a checkbox for inclusion of the subcategory in the Profile and a button for viewing the subcategory's description.
- A non-editable text field showing an XML representation of the Profile.

Figure 14 shows the Framework Profile tab. The user can determine which subcategories are in the Profile by checking or unchecking the box to the left of the subcategory's button. Any subcategory added to the Profile by clicking the Cyber Framework Browser tab's "Add to Profile" button (see Figure 3) will have a checkmark. Clicking on a subcategory button causes the user interface to switch to the Cyber Framework Browser tab, with the "Subcategory" drop-down value set to the button's subcategory, the "Category" drop-down value set to the category to which the subcategory belongs, and the "Framework core function" radio button selection set to the function to which the category belongs. For example, suppose a user were to click on the button in Figure 14 with label PR.AC-1. This would result in the user interface appearing as in Figure 3.

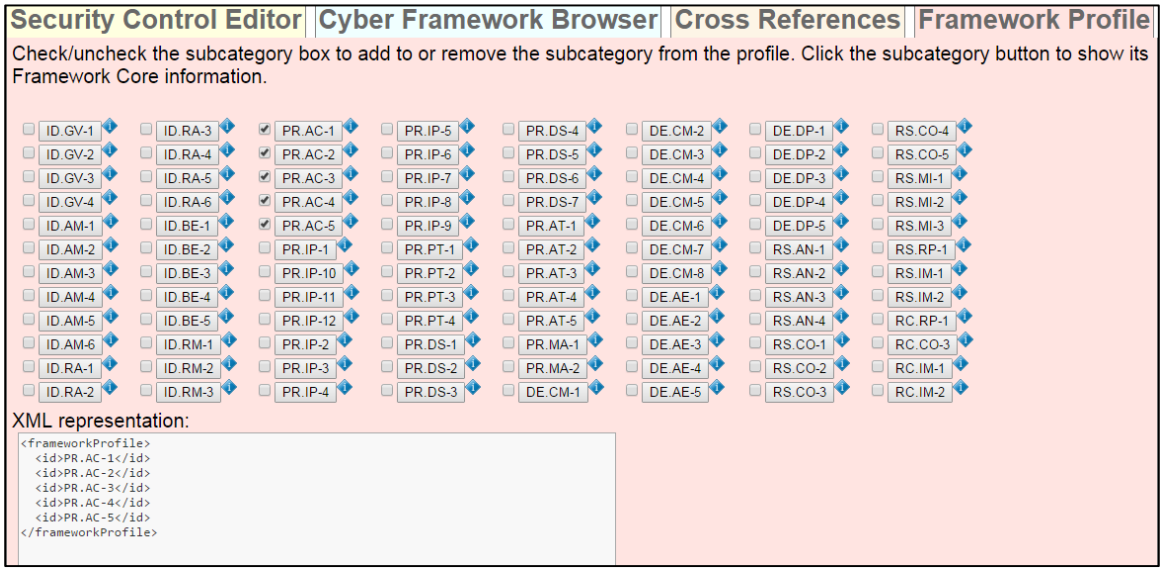


Figure 14. Framework Profile tab.

The Profile shown in Figure 14 contains all five subcategories of category PR.AC. If the "Restrict controls to Framework Profile informative references" box in the Security Control Editor tab is checked (as shown in Figure 16 and Figure 17), then the Security Control Editor's "Control family" and "Control" drop-down choices will be restricted to only those controls referenced by the subcategories of PR.AC.

The non-editable "XML representation" text field at the bottom of Figure 14 shows XML updated on the fly based on which subcategory checkboxes are checked. As with the XML generated in the Security Control Editor tab, this XML can be copy-pasted into a third-party authoring application.

4 Bringing it All Together

Section 3 covered the first three Baseline Tailor usage scenarios in the bulled list at the beginning of section 1: security control tailoring, Framework Profile development, and generation of XML output. This section discusses the fourth scenario: coherently synthesizing

the guidance from the Framework Core, NIST SP 800-53 security control catalog, and NIST SP 800-82 ICS overlay. Without Baseline Tailor, an individual wishing to use these specifications together would have to deal with three separate information sources, each organized differently. Baseline Tailor's user interface makes it easier to use the specifications together. Additionally, Baseline Tailor provides new information derived through integrating the disparate information sources – information not obvious from studying each specification in isolation.

The flowchart in Figure 15 shows a possible Baseline Tailor workflow for the fourth scenario. The user begins by creating a Profile containing a set of Framework Core subcategories needed to meet a cybersecurity requirement. Next, the user considers each of the Profile's informative references. For each security control referenced, the user performs the following actions to determine how critical the security control is to achieving the Profile's outcomes:

- Checks how many of the Profile's subcategories reference the security control.
- Views the security control's NIST SP 800-53 database definition to determine relevance.

If the user deems the security control to be critical for meeting the cybersecurity requirement, the user then proceeds to tailor the security control. The user may apply the NIST SP 800-82 Industrial Control System overlay tailoring guidance, if applicable, as a starting point.

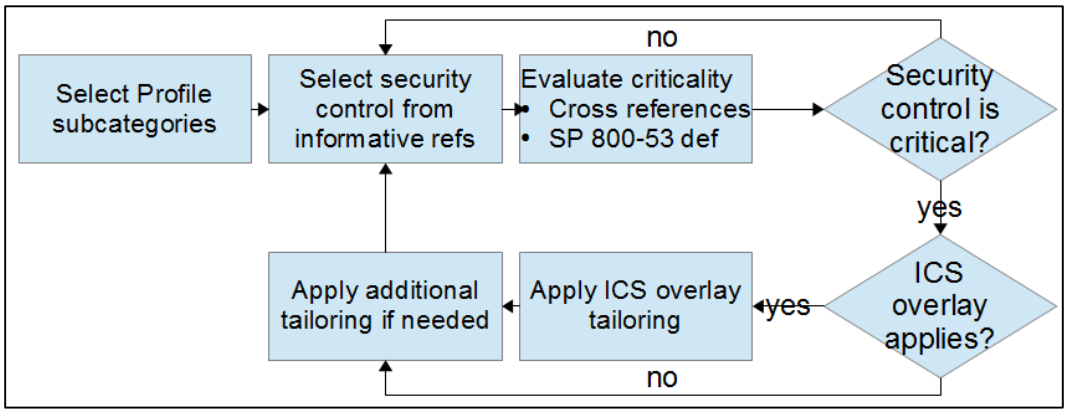


Figure 15. Workflow synthesizing Framework Core, NIST SP 800-53, and NIST SP 800-82 guidance.

As a concrete example of the workflow in Figure 15, suppose a cybersecurity analyst wants to protect a Distributed Control System (DCS) from unauthorized access. A DCS is a type of ICS commonly used to regulate production systems within a manufacturing facility. The analyst decides to use Baseline Tailor to help determine which security controls should be selected and tailored for implementation. The analyst begins by checking the NIST SP 800-82 checkbox in the preferences dialog (shown in Figure 2). In the Cyber Framework Browser tab, the analyst then chooses the PROTECT (PR) core function and Access Control (PR.AC) category (shown in Figure 3). Using the Subcategory drop-down list, the analyst next looks at PR.AC's five subcategories and decides to create a Profile containing all of them. To do so, the analyst switches to the Framework Profile tab and makes the checkbox selections shown in Figure 14.

The analyst now switches to the Security Control Editor tab and checks the box restricting control choices to only those that are referenced by subcategories of PR.AC. As shown in Figure 16, The PR.AC subcategories reference only four of the eighteen NIST SP 800-53 control families. Now suppose the analyst selects ACCESS CONTROL from the "Control family" drop-down list, and then chooses "AC-2 – ACCOUNT MANAGEMENT" from the "Control" drop-down list populated with the subset of the Access Control family that the Profile references (Figure 17). The Security Control Editor tab now displays the user interface for tailoring AC-2, the upper portion of which is shown in Figure 18.

At this point, the analyst wishes to determine security control AC-2's criticality with respect to Framework Core category PR.AC. Clicking the "Framework Core Subcategories Referencing AC-2" button in Figure 16 reveals that two of the five PR.AC subcategories – PR.AC-1 and PR.AC-4 – reference AC-2 (shown in Figure 13). Concluding that security control AC-2 should be selected for implementation, the analyst clicks the AC-2 button shown in the upper left of Figure 18 to look up AC-2's definition in the NIST SP 800-53 database. NIST SP 800-53 gives AC-2 a priority of P1 (Figure 19). Also, items *d*, *i*, and *k* in the AC-2 Control Description (Figure 20) are relevant to category PR.AC. The analyst therefore decides to go ahead and tailor AC-2 for Distributed Control Systems.

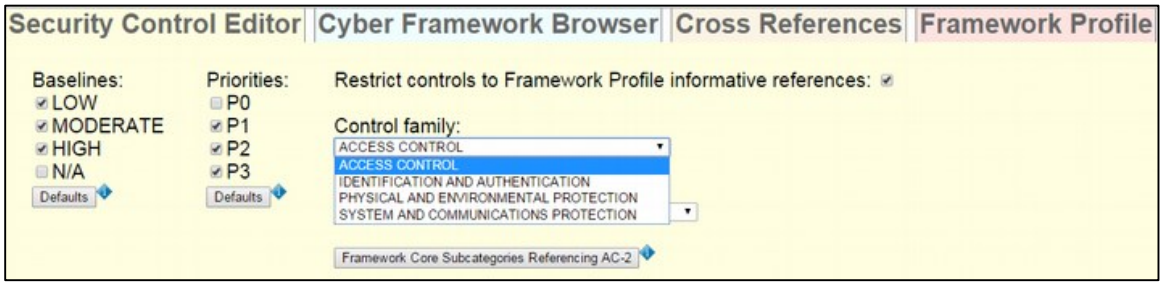


Figure 16. Control families referenced by PR.AC subcategories.

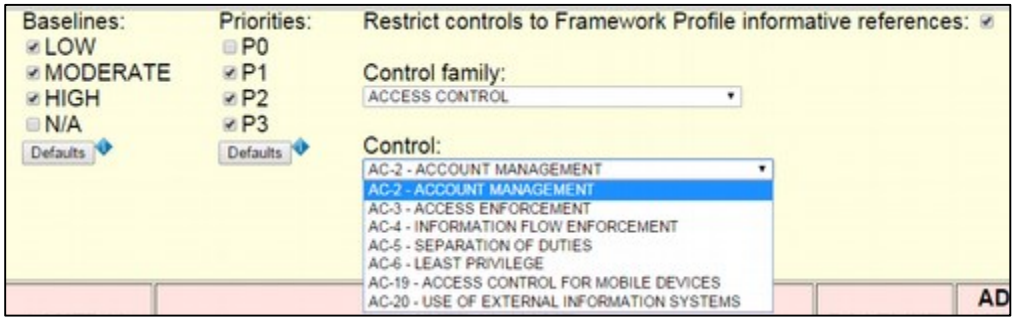


Figure 17. Controls belonging to Access Control family that are referenced by PR.AC subcategories.

The analyst now clicks on the button with the factory image in Figure 18, to the right of the AC-2 button, to view AC-2's tailoring guidance in the NIST SP 800-82 Industrial Control System overlay. The overlay guidance (Figure 21) retains the same baseline allocation as NIST SP 800-53, but adds ICS-specific supplemental guidance suggesting compensating controls.

Compensating controls are alternatives, for when the NIST SP 800-53 recommendations are not feasible, that provide comparable protection. The compensating controls mentioned in Figure 21 meet requirements specific to ICS. For example, an ICS may have limited network connectivity and only a small number of potential users, making physical security measures possibly more cost-effective than account management (where information processing overhead might impact performance). Using the NIST SP 800-82 guidance as a starting point, the analyst proceeds to tailor AC-2 using Baseline Tailor's Security Control Editor tab.

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

Figure 18. Security control AC-2.

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

Figure 19. NIST SP 800-53 database: AC-2 summary.

To summarize, the scenario discussed in this section shows how Baseline Tailor can increase the utility of the Framework Core, NIST SP 800-53 database, and NIST SP 800-82 ICS overlay. Baseline Tailor not only provides a single user interface bringing them all together, but also derives important inter-relationships. As the example showed, a Framework Profile can be used to limit the Security Control Editor tab's "Control family" and "Control" drop-down choices to the subset of NIST SP 800-53 security controls likely to be most relevant to the Profile. Also, the Cross References tab can be used as a metric for a security control's importance with respect to the Framework Core.

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.

Figure 20. NIST SP 800-53 database: AC-2 description.

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.

Figure 21. NIST SP 800-82 ICS Overlay definition: AC-2.

5 XML Formats

Baseline Tailor produces two types of XML data: data representing a Framework Profile and data representing a tailored security control. The Framework Profile XML format shown in

Figure 14 is very simple. Its representation is limited to only the identifier of each subcategory included in the Profile.[7] The tailored security control XML format shown in Figure 11 is more information-intensive. Consider the IA-3 example from subsection 3.2. The XML data produced represents not only all changes to the NIST SP 800-53 IA-3 baseline, but also the rationale explaining why the baseline was changed and ICS-specific supplemental guidance for the control and two of its enhancements.

Neither of these two XML formats are particularly useful in isolation. Although they contain information pertaining to selection and tailoring, the formats do not represent the content of what is being selected or tailored. For the Framework Profile XML representation, the missing piece is XML representing the Framework Core content. For the tailored security control XML, the missing piece is XML representing the NIST SP 800-53 security control catalog content.

Fortunately, these two "missing" pieces are not actually missing. Baseline Tailor uses an XML representation of the Framework Core internally to populate the user interface objects in Cyber Framework Browser tab (discussed in 3.1). An XML representation of the NIST SP 800-53 security control catalog powers the NIST SP 800-53 database (mentioned in section 1). Thus, when supplemented with the Framework Core and security catalog XML data sources, the XML Baseline Tailor produces provides a useful representation of a Profile or tailored control.

Links to the aforementioned XML resources, including annotated schemas for validation, are available at https://github.com/usnistgov/sctools.

6 Concluding Remarks

This guide documented the Baseline Tailor software application and discussed some usage scenarios. These examples are not exhaustive. Many organizations – public as well as private sector – use the Cybersecurity Framework, NIST SP 800-53, and NIST SP 800-82 specifications. As these organizations gain experience with the specifications, and as new groups turn to them in response to an ever-increasing cyber threat landscape, additional potential uses for Baseline Tailor are likely to emerge.

Although Baseline Tailor has proven itself useful for internal NIST projects, the current implementation has a number of known issues. Section 5 mentioned one of them, the paucity of the Framework Profile XML representation. Another issue is an inability to import an existing tailored control. Such a feature would enable composability, for example performing additional tailoring on a control from the NIST SP 800-82 overlay. A third limitation is lack of support for NIST SP 800-53 assignment and selection parameters, which allow organizations to define organization-specific values associated with controls. A more complete list of issues, including bugs, is available on GitHub at https://github.com/usnistgov/sctools.

All three of the NIST specifications Baseline Tailor supports – the Cybersecurity Framework, NIST SP 800-53, and NIST SP 800-82 – receive periodic updates in response to public

[7] A future version of Baseline Tailor may support a more information-rich Framework Profile XML format. Such a format might include, for example, guidance for subcategories in the Profile.

comments, new research results, and implementation experience. Indeed, as of April 2016, work on the next version of NIST SP 800-53 is underway [10], and NIST is in the midst of determining how to further advance the Cybersecurity Framework.[8] Any upcoming modifications to the Framework Core, security control catalog, NIST SP 800-53 tailoring methodology, or ICS overlay would likely require that corresponding changes be made to Baseline Tailor implementation to maintain compatibility.

Baseline Tailor is a research prototype whose underlying purpose is to spur development of third-party software products that aid users of the Cybersecurity Framework and NIST SP 800-53 security controls. Would-be software developers are encouraged to obtain and experiment with the source code, available at https://github.com/usnistgov/sctools. For questions about the code, or about Baseline Tailor in general, please email the point of contact listed on the Baseline Tailor information page at http://www.nist.gov/el/msid/baselinetailor.cfm. Feedback, bug reports, and suggestions for improvement are all welcome. The Baseline Tailor information page also contains links to publications and presentations discussing implementation details not covered in this document.

[8] NIST received numerous comments [11] in response to a Request for Information (RFI) [12] issued in December of 2015.

References

[1] National Institute of Standards and Technology (NIST) and United States of America, "Framework for Improving Critical Infrastructure Cybersecurity," 2014.

[2] Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology, NIST SP 800-53r4, Apr. 2013.

[3] "Extensible Markup Language (XML) 1.0 (Fifth Edition)," *W3C Recommendation*, 26-Nov-2008. [Online]. Available: http://www.w3.org/TR/xml/.

[4] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," *NIST Special Publication 800-82 Revision 2*, May 2015.

[5] A. Mesbah and A. van Deursen, "Migrating Multi-page Web Applications to Single-page AJAX Interfaces," *11th European Conference on Software Maintenance and Reengineering, 2007*, pp. 181–190, Mar. 2007.

[6] "ECMAScript 2015 Language Specification," Ecma International, Standard ECMA-262, Jun. 2015.

[7] "Hypertext Transfer Protocol - HTTP/1.1," Internet Engineering Task Force, RFC 2616, Jun. 1999.

[8] "NVD - 800-53." [Online]. Available: https://web.nvd.nist.gov/view/800-53/home.

[9] "XSL Transformations (XSLT) Version 1.0," *W3C Recommendation*, 16-Nov-1999. [Online]. Available: http://www.w3.org/TR/xslt.

[10] "NIST Computer Security Publications - Drafts." [Online]. Available: http://csrc.nist.gov/publications/PubsDrafts.html#800-53r5. [Accessed: 01-Apr-2016].

[11] "RFI - Framework for Reducing Cyber Risks to Critical Infrastructure." [Online]. Available: http://csrc.nist.gov/cyberframework/rfi_comments_02_09_16.html. [Accessed: 01-Apr-2016].

[12] "Federal Register | Views on the Framework for Improving Critical Infrastructure Cybersecurity." [Online]. Available: https://www.federalregister.gov/articles/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity. [Accessed: 01-Apr-2016].