**NISTIR XXXX**

**Baseline Tailor User Guide**

Joshua Lubell

This publication is available free of charge from:

http://dx.doi.org/10.6028/NIST.IR.XXXX





**NISTIR XXXX**

**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.XXXX

Month and Year of Publication



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*

# Preface

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 can be found 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 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 that are 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 NIST’s GitHub team for their support in deploying Baseline Tailor.

# Introduction

This guide describes how to use Baseline Tailor, a software tool for navigating the United States government’s Cybersecurity Framework [1] and for tailoring the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 [2] security controls. Baseline Tailor generates output in Extensible Markup Language (XML) [3] formats capturing a user’s Framework Profile and tailoring choices.

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. The baselines are suggested defaults for “typical” information systems. 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.

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, helping to 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.

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.
* Section 4 presents a usage 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 some guidance on using the XML data Baseline Tailor generates.

# 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. Baseline Tailor also runs, albeit slowly, in Internet Explorer.

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, but 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.

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>).

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 <https://github.com/usnistgov/sctools>, 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 installation should start up Chrome with the --allow-file-access-from-files 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 a workaround, users can instead refer to the security control catalog in Appendix F of the NIST SP 800-53 document.

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

# User Interface

The Baseline Tailor user interface has four tabs:

* A Cyber Framework Browser tab for navigating the Framework Core.
* A Security Control Editor tab for navigating the NIST SP 800-53 security control catalog and tailoring controls.
* A Framework Profile tab 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” pushbutton above the tabs, shown in Figure 1, to turn certain Baseline Tailor features on or off. Clicking the pushbutton 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” pushbutton to hide the dialog.



Figure 1. Preferences pushbutton above user interface tabs.



Figure 2. Preferences dialog.

The following subsections describe the four Baseline Tailor user interface tabs in detail, using as an 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.

## Cybersecurity Framework Browser

The Cybersecurity 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 pushbutton 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:
  + Pushbuttons for NIST SP 800-53 database and NIST SP 800-82 ICS overlay lookup of the referenced security control.
  + A pushbutton for showing all Framework Core subcategories that also reference the security control.
  + A pushbutton 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.

Underneath the description of subcategory PR.AC-1 is an “Add to profile” pushbutton the user can click on to add PR.AC-1 to the current Framework Profile. If PR.AC-1 had already been added, the pushbutton 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 3.4.

The bottom portion of Figure 3 contains pushbuttons 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 pushbuttons to search the NIST SP 800-53 online database in a new Internet browser tab[[1]](#footnote-1). Clicking the pushbutton with the factory image produces a new Internet browser tab with the ICS overlay definition for AC-2[[2]](#footnote-2). The user may view all the other Framework Core subcategories that reference AC-2 by clicking the pushbutton with the link image. Doing so causes the user interface to switch to the Cross References tab (described in 3.3). The user may tailor security control AC-2 by clicking on the pushbutton with the needle-and-thread image[[3]](#footnote-3). Doing so causes the user interface to switch to the Security Control Editor tab (described in 3.2).

## Security Control Editor

The Security Control Editor tab, the most complex of Baseline Tailor’s user interface tabs, supports the following operations in accordance with NIST SP 800-53 tailoring guidelines:

* 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.

Figure 4 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 pushbuttons to the left are for restricting the choices in the control drop-down list based on the NIST SP 800-53 baseline impact and/or priority. Checking the upper right checkbox restricts the 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” pushbutton underneath the control drop-down list changes the focus to the Cross References tab (described in 3.4).

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 4. The two leftmost columns contain the identifier and name for the control and each of its enhancements. The control identifier appears as a pushbutton 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 pushbutton 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. A drop-down value of LOW indicates the control or enhancement is included in all baselines. MODERATE indicates moderate and high baselines only. HIGH indicates high baseline only. N/A indicates the control or enhancement is excluded from all baselines.

The values shown in Figure 4 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, and excludes IA-3's enhancements from all three default baselines. 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 checkbox in the fourth column allows the user to provide additional supplemental guidance, beyond that given in NIST SP 800-53, for the control.



Figure 4. Security control IA-3.

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. “Selected” indicates the control or enhancement is in the NIST SP 800-53 baseline and has not been tailored out. “Added” indicates the user has tailored in the control or enhancement. “Removed” indicates the control or enhancement has been tailored out. No entry indicates that 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 5 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 6 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 7 shows the result when a user attempts to add supplemental guidance to a control enhancement before adding the control enhancement to a baseline.



Figure 5. Violation of baseline impact constraint.



Figure 6. Violation of cross-reference constraint.



Figure 7. Violation of baseline constraint.

Now suppose a user tailors IA-3 for Industrial Control Systems as per the NIST SP 800-82 overlay. Since an Industrial Control System (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 8. IA-3 tailored for an Industrial Control System.

Figure 8 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.

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 8, the editable text fields contain stub text. Figure 9 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 4 provides additional details on the XML formats Baseline Tailor generates.



Figure 9. IA-3 text fields with ICS-specific guidance replacing stubs.

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 10 shows how the copy-pasted result might look. The Baseline Tailor distribution includes XML schemas (discussed in Section 4) for use with third-party XML authoring tools.



Figure 10. XML generated by the Security Control Editor copy-pasted into a third party XML authoring software application.

## Cross References

The Baseline Tailor user interface provides two ways a user can display all Framework Core subcategories referencing a particular security control. The first way, discussed in 3.1, is by clicking a pushbutton in the Cyber Framework Browser tab with a link image. The second way, discussed in 3.2, is by clicking on the “Framework Core subcategories referencing…” pushbutton in the Security Control Editor tab. Performing either action changes the focus to the Cross References tab.

The Cross References tab shows all Framework Core subcategories referencing whichever security control was most recently selected – either by clicking a pushbutton with a link image in the Cyber Framework Brower tab or by clicking the “Framework Core subcategories referencing…” pushbutton in the Security Control Editor tab. The Cross References tab displays the subcategories as pushbuttons, which may be clicked to display the subcategory in the Cyber Framework Browser tab.

Suppose the Security Control Editor tab appears as shown in Figure 4, and the user has clicked the “Framework Core subcategories referencing IA-3” pushbutton. Then the Cross References tab would appear as shown in Figure 11. As the figure shows, PR.AC-1 is the only subcategory referencing IA-3. Clicking the PR.AC-2 pushbutton 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 11. Subcategory referencing IA-3.

Figure 12 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” pushbutton. As Figure 12 shows, four Framework Core subcategories reference AC-2. Clicking any of these subcategory pushbuttons causes a focus change to the Cyber Framework Browser tab, with the appropriate widget selections.



Figure 12. Subcategories referencing AC-2.

## Framework Profile



Figure 13. Framework Profile tab.

The Framework Profile tab, shown in Figure 13, allows users to add any subcategory to or remove any subcategory from the current Framework Profile. There are pushbuttons for every Framework Core subcategory. The user can determine which subcategories are in the Profile by checking or unchecking the box to the left of the subcategory’s pushbutton. Any subcategory added to the Profile by clicking the Cyber Framework Browser tab’s “Add to Profile” pushbutton (see Figure 3) will have a checkmark. Clicking on a subcategory pushbutton causes the user interface to switch to the Cyber Framework Browser tab, with the “Subcategory” drop-down value set to the pushbutton’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 pushbutton in Figure 13 with label PR.AC-1. This would result in the user interface appearing as in Figure 3[[4]](#footnote-4).

The Profile shown in Figure 13 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, 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 13 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.

# Bringing it All Together

Section 3 covered two Baseline Tailor usage scenarios: security control tailoring and Framework Profile development. Another use for Baseline Tailor is as a tool for synthesizing into a coherent whole the security 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.

For example, suppose a cybersecurity analyst wants to protect a Distributed Control System, a type of Industrial Control System commonly used to regulate production systems within a manufacturing facility, from unauthorized access. 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 13.

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 14, 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 15). The Security Control Editor tab now displays the user interface widgets for tailoring AC-2, the upper portion of which are shown in Figure 16.



Figure 14. Control families referenced by PR.AC subcategories.



Figure 15. Controls belonging to Access Control family that are referenced by PR.AC subcategories.



Figure 16. Security control AC-2.

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” pushbutton in Figure 14 reveals that two of the five PR.AC subcategories – PR.AC-1 and PR.AC-4 – reference AC-2 (shown in Figure 12). Concluding that security control AC-2 should be selected for implementation, the analyst clicks the AC-2 pushbutton shown in the upper left of Figure 16 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 17). Also, items *d*, *i*, and *k* in the AC-2 Control Description (Figure 18) are relevant to category PR.AC. The analyst therefore decides to go ahead and tailor AC-2 for Distributed Control Systems.



Figure 17. NIST SP 800-53 database: AC-2 summary.



Figure 18. NIST SP 800-53 database: AC-2 description.



Figure 19. NIST SP 800-82 ICS Overlay definition: AC-2.

The analyst now clicks on the pushbutton with the factory image in Figure 16, to the right of the AC-2 pushbutton, to view AC-2’s tailoring guidance in the NIST SP 800-82 Industrial Control System overlay. The overlay guidance (Figure 19) 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 19 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.

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.

# 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 13 is very simple. Its representation is limited to only the identifier of each subcategory included in the Profile[[5]](#footnote-5). The tailored security control XML format shown in Figure 10 is more information-intensive. Consider the IA-3 example from 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 format does 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://pages.nist.gov/sctools>.

# 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.

1. 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. [↑](#footnote-ref-1)
2. This pushbutton appears only if the NIST SP 800-82 overlay box in the preferences dialog is checked. [↑](#footnote-ref-2)
3. This pushbutton appears only if the Security Control Editor tab box in the preferences dialog is checked. [↑](#footnote-ref-3)
4. Except that, instead of an “Add to Profile” pushbutton appearing below the PR.AC-1 description, there would be a “Remove from Profile” pushbutton. [↑](#footnote-ref-4)
5. 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. [↑](#footnote-ref-5)