# Introduction

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

The primary goals of the Baseline Tailor are to:

* Make it easy to create tailored baseline documentation.
* Enforce constraints on tailoring operations, helping to ensure that the result follows NIST SP 800-53 guidelines.
* Generate XML valid with respect to a schema for tailored controls that can be used in conjunction with NIST SP 800-53 XML data and other XML-encoded security content to achieve security automation.

Baseline Tailor is a single-page web application [4]. Single-page applications, also known as AJAX (Asynchronous JavaScript [5] 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 without a Hypertext Transfer Protocol (HTTP) [6] server in browsers that that do not block read access to local files.

The Baseline Tailor user interface (discussed in Section 4) provides context-sensitive search of the NIST SP 800-53 database [7], an online version of the security catalog from the NIST SP 800-53 Revision 4 document. The search function enables the user to conveniently look up the definition and guidance for the currently selected security control, or for security controls referenced by the currently Framework Core selection.

Baseline Tailor adopts a minimalist approach. The software neither creates nor modifies any files. Instead, Baseline Tailor displays its output in a multiple-line, resizable text field. The user can copy-paste this output into a third party XML editing application. Baseline Tailor’s inability to 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.

# Disclaimers

Any mention of commercial or other third party products in this user 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 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.

# Getting Started

Baseline Tailor requires an Internet browser with support for JavaScript and the Extensible Stylesheet Language Transformations (XSLT) 1.0 standard [8]. Most of today’s common browsers meet this requirement. Although not required, software for editing XML documents is desirable. It is possible to copy-paste Baseline Tailor’s output into a plain text editor for further modification, but XML editing software is easier to use, supports validation against a schema, and may also include other useful XML-specific functionalities.

Baseline Tailor users should understand the content of NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [2], particularly Chapter Three which discusses how to select and specify security controls. This document and other information security standards, guidelines, and resources are available online from NIST’s Computer Security Resource Center (<http://csrc.nist.gov>).

Baseline Tailor users may also wish to read the *Framework for Improving Critical Infrastructure Cybersecurity* [1], also available from the Computer Security Resource Center, for guidance on using the Framework Core in conjunction with NIST SP 800-53.

Baseline Tailor is distributed as a zip file, downloadable from the NIST website. To install, unzip the zip file. To run Baseline Tailor, open the file bt.xml in an Internet browser.

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, Google 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 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, a user can instead refer to the security control catalog in Appendix F of the NIST SP 800-53 document.

# User Interface

The Baseline Tailor user interface has three tabs:

* A Security Control Editor tab for navigating the NIST SP 800-53 security control catalog and tailoring controls.
* A Cyber Framework Browser tab for navigating the Framework Core.
* A Cross References tab shows all references from the Framework Core to the control currently selected in the Security Control Editor tab.

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

The following subsections describe each of these tabs in detail.

## Security Control Editor

The Security Control Editor tab supports the following operations in accordance with NIST SP 800-53 tailoring guidelines:

* Adding or removing controls or control enhancements in a baseline. SP 800-53 requires documenting the rationale for modifying the baseline.
* Adding additional guidance to a control or control enhancement.

Figure 1 shows the upper portion of the Security Control Editor tab before any tailoring has been initiated. The two drop-down lists in the upper right hand corner are for choosing an individual control from a control family. The user has chosen security control IA-3 (Device Identification and Authentication) from the Identification and Authentication family. The checkboxes and buttons to the left are for restricting the choices in the control pulldown based on the NIST SP 800-53 default baseline impact and/or priority.

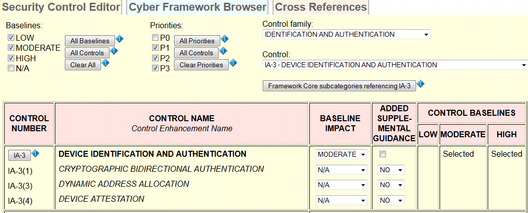


Figure 1. Security control IA-3.

Paragraph.

Paragraph.

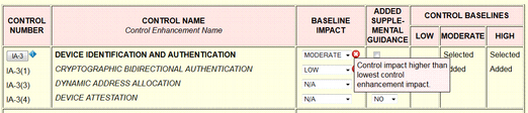


Figure 2. Violation of baseline impact constraint.

Paragraph.

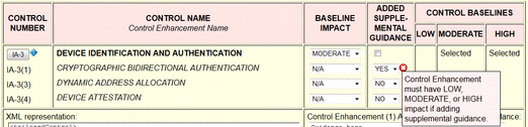


Figure 3. Violation of baseline constraint.

Paragraph.

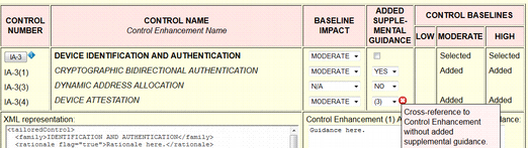


Figure 4. Violation of cross-reference constraint.

Paragraph.

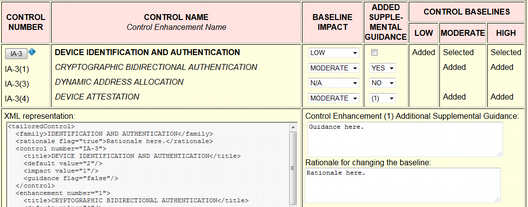


Figure 5. IA-3 tailored for an Industrial Control System.

Paragraph.

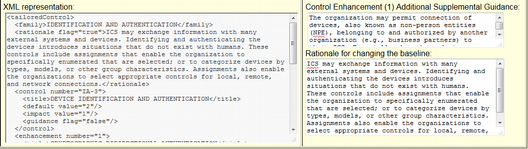


Figure 6. IA-3 Rationale and guidance text added.

Paragraph.

<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 specifically enumerated that are selected; or 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="false"/>

</control>

<enhancement number="1">

<title>CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION</title>

<default value="4"/>

<impact value="2"/>

<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>

</enhancement>

<enhancement number="4">

<title>DEVICE ATTESTATION</title>

<default value="4"/>

<impact value="2"/>

<guidance flag="1"/>

</enhancement>

</tailoredControl>

Figure 9. Full XML data generated by the Security Control Editor.

Paragraph.

## Cybersecurity Framework Browser

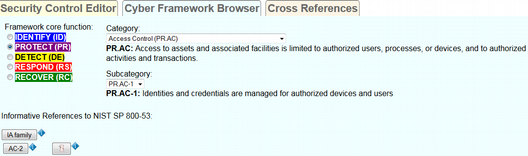


Figure 8. Framework Core subcategory referencing the IA control family.

## Cross References

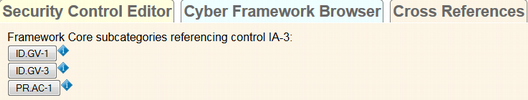


Figure 9. IA-3 cross references to Framework Core.

# 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] A. Mesbah and A. van Deursen, “Migrating Multi-page Web Applications to Single-page AJAX Interfaces,” *Software Maintenance and Reengineering, 2007. CSMR ’07. 11th European Conference on*, pp. 181–190, Mar. 2007.

[5] “ECMAScript 2015 Language Specification,” Ecma International, Standard ECMA-262, Jun. 2015.

[6] “Hypertext Transfer Protocol - HTTP/1.1,” Internet Engineering Task Force, RFC 2616, Jun. 1999.

[7] “NVD - 800-53.” [Online]. Available: https://web.nvd.nist.gov/view/800-53/home.

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