# 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.

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 offline without a Hypertext Transfer Protocol (HTTP) [6] server in browsers that that do not block read access to local files.

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.

# Getting Started

The only requirement for using Baseline Tailor is an Internet browser with support for JavaScript and the Extensible Stylesheet Language Transformations (XSLT) 1.0 standard [7]. Most of today’s common browsers meet this requirement. Although not required, software for editing XML documents is desirable. Although it is possible to copy-paste Baseline Tailor’s output into a plain text editor for further modification, XML editing software allows is easier to use, supports validation against a schema, and may also include other useful XML-specific features.

Running over HTTP.

Running from local files.

# User Interface

Paragraph.

## Cybersecurity Framework Browser

## Security Control Editor

Paragraph.

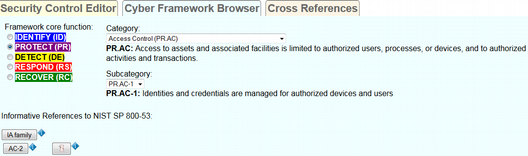


Figure 1. Framework Core subcategory referencing the IA control family.

Paragraph.

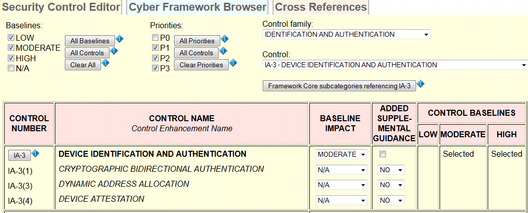


Figure 2. Security control IA-3.

Paragraph.

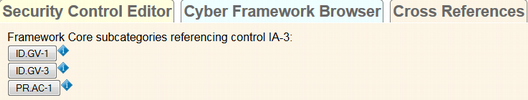


Figure 3. IA-3 cross references to Framework Core.

Paragraph.

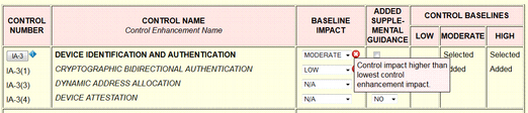


Figure 4. Violation of baseline impact constraint.

Paragraph.

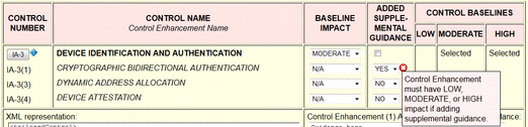


Figure 5. Violation of baseline constraint.

Paragraph.

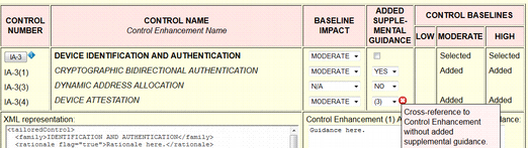


Figure 6. Violation of cross-reference constraint.

Paragraph.

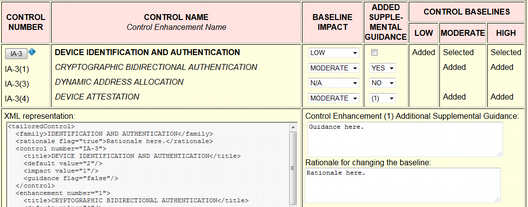


Figure 7. IA-3 tailored for an Industrial Control System.

Paragraph.

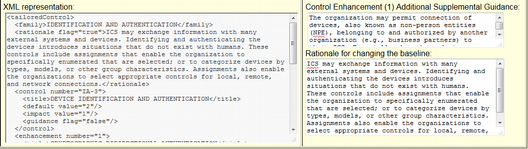


Figure 8. IA-3 Rationale and guidance text added.

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.

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