**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*

# Introduction

This guide describes how to use Baseline Tailor, a software tool for using 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 an Extensible Markup Language (XML) [3] format 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 provides 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 and/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 includes 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 the 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 4) provides context-sensitive search of the NIST SP 800-53 database [8], an online version of the NIST SP 800-53 Revision 4 security catalog. 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 current 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 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 [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 [URL here], 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, a user 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 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, 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 the NIST SP 800-82 overlay.

## Cybersecurity Framework Browser

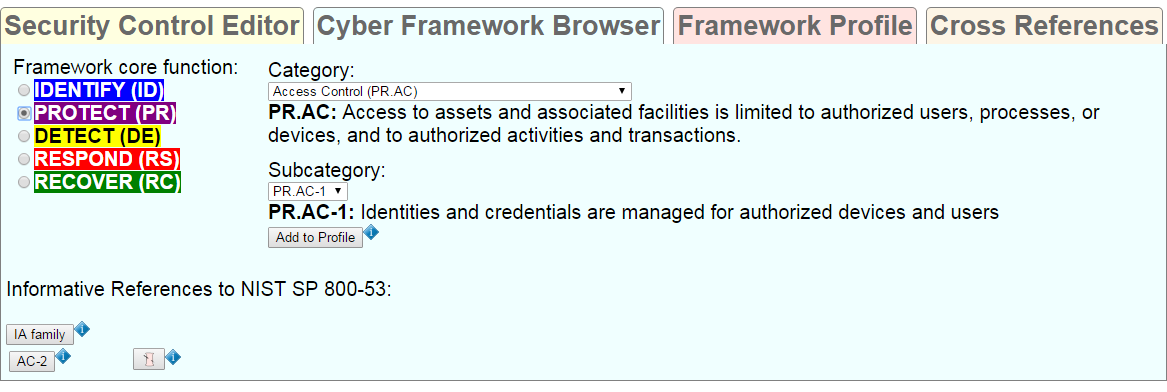


Figure 1. Framework Core subcategory referencing the IA control family.

## 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 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 2 shows the upper portion of the Security Control Editor tab after the user has selected security control IA-3, but 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 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/or priority. 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 underneath the control drop-down list changes the focus to the Cross References tab (described in 4.3).

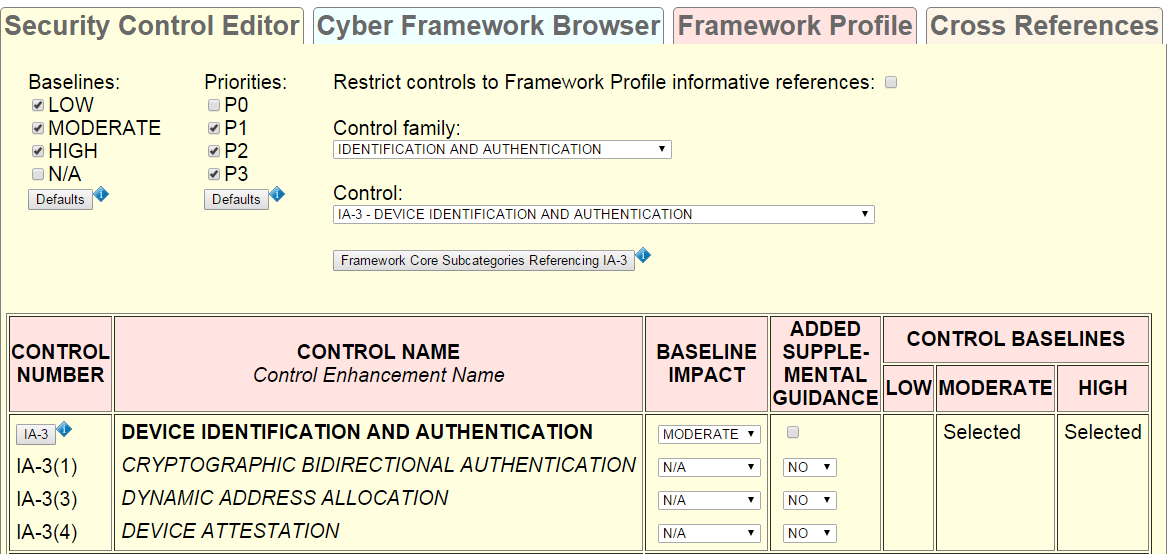


Figure . Security control IA-3.

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. 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. 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 2 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.

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 3 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 4 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 5 shows the result when a user attempts to add supplemental guidance to a control enhancement before adding the control enhancement to a baseline.

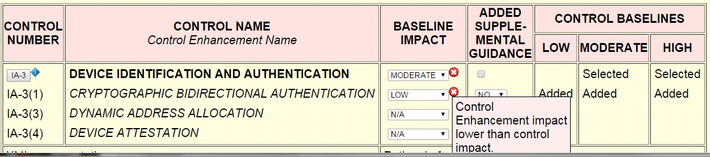


Figure . Violation of baseline impact constraint.

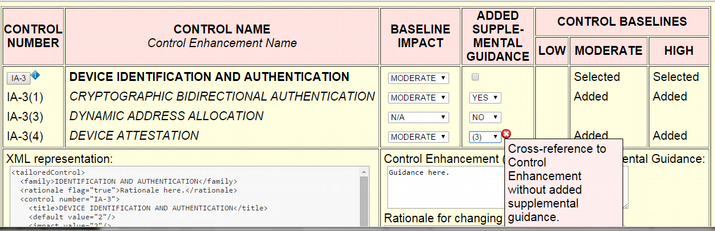


Figure . Violation of cross-reference constraint.

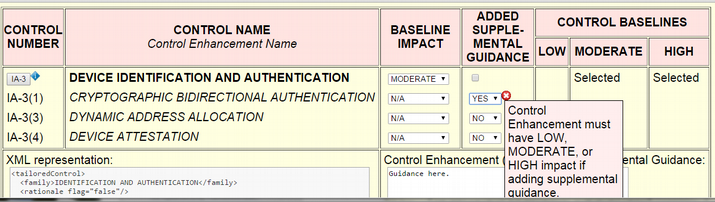


Figure . Violation of baseline constraint.

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 6 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.

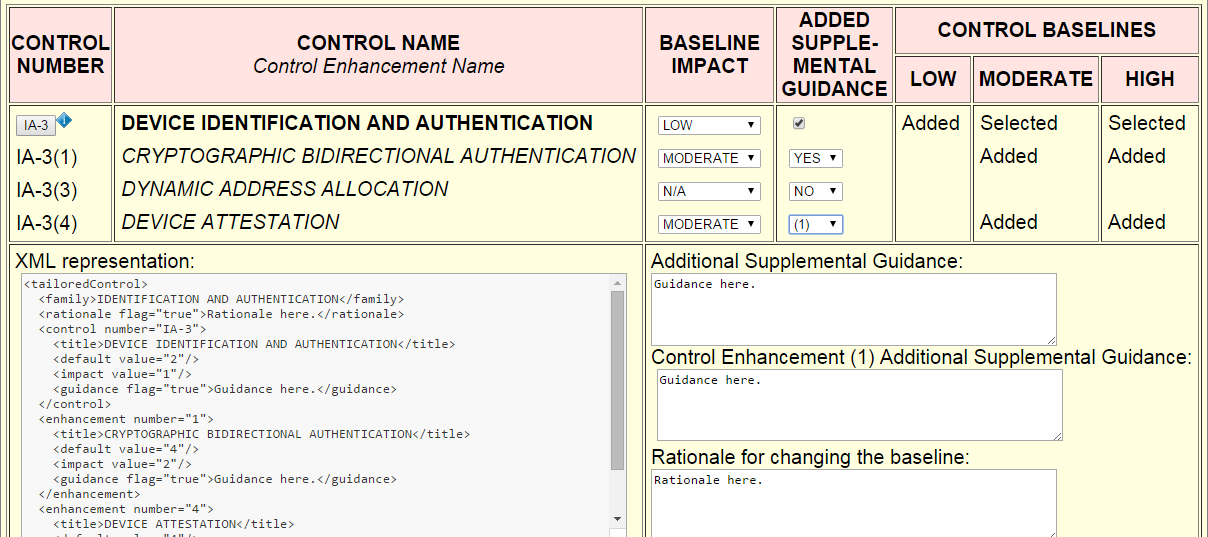


Figure . IA-3 tailored for an Industrial Control System.

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 6, the editable text fields “XML representation” text field contain stub text. Figure 7 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 describes the XML format Baseline Tailor generates in further detail.



Figure . 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 8 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.

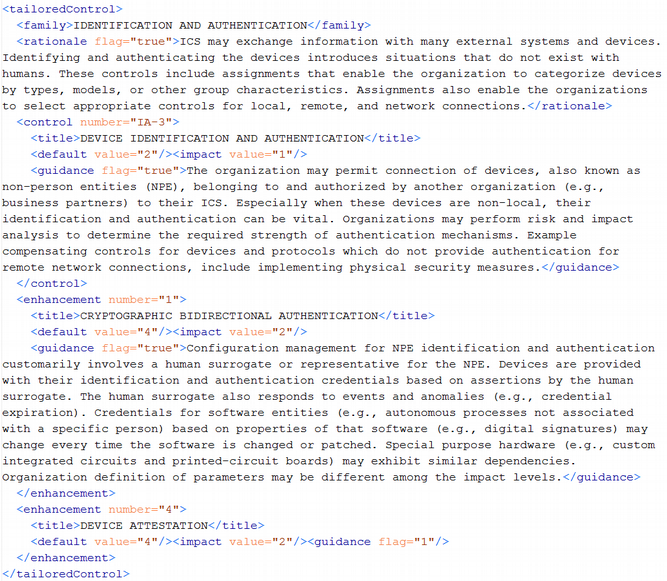


Figure 8. XML generated by the Security Control Editor copy-pasted into a third party XML authoring software application.

## Framework Profile

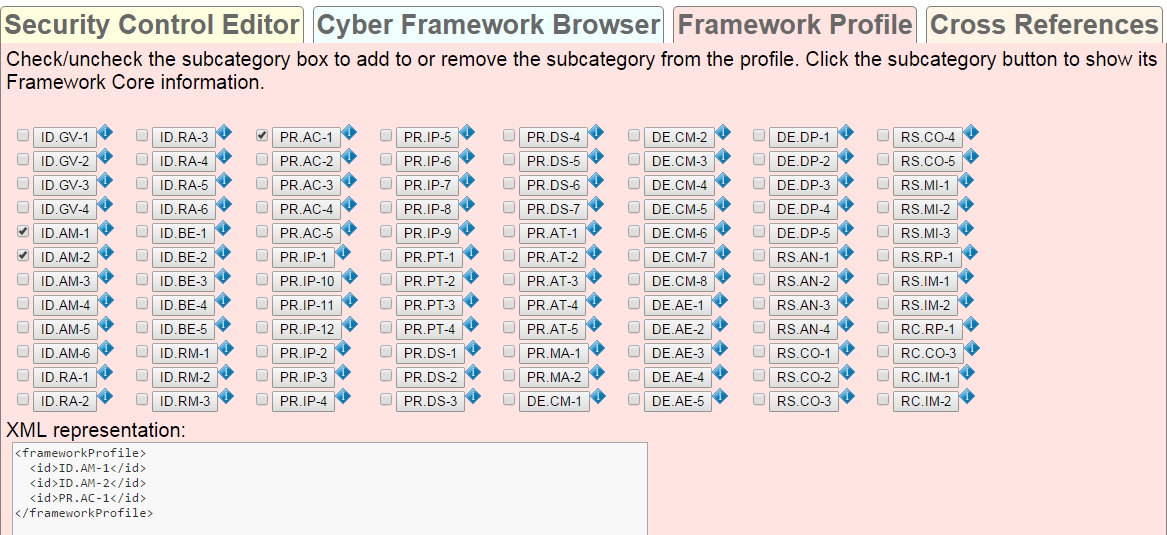


Figure 9. Framework Profile tab.

## Cross References

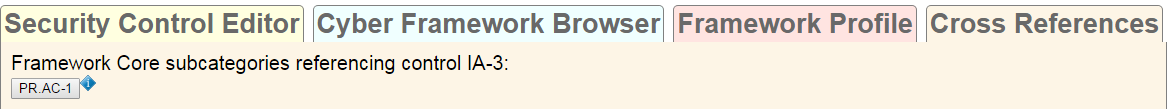


Figure . IA-3 cross references to Framework Core.

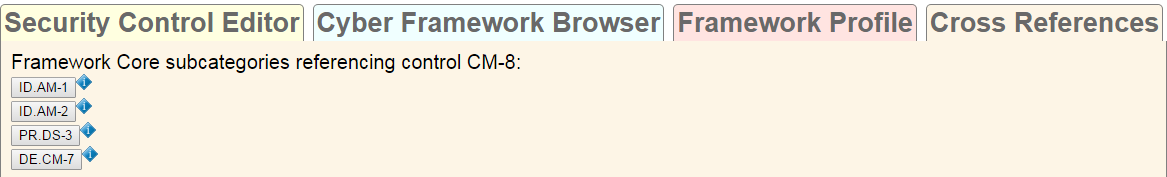


Figure 11. CM-I cross references to Framework Core.

# XML Formats for Framework Profiles and Tailored Controls

# Possible Future Directions

# 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,” *Software Maintenance and Reengineering, 2007. CSMR ’07. 11th European Conference on*, 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.