Volume 123, Article No. 123007 (2018) https://doi.org/10.6028/jres.123.007
Journal of Research of the National Institute of Standards and Technology

Baseline Tailor

Joshua Lubell

National Institute of Standards and Technology,
Gaithersburg, MD 20899, USA

joshua.lubell@nist.gov

Software DOI: https://doi.org/10.18434/T4/1422488

Software Version: 0.11

Key words: cybersecurity framework; industrial control system; security control; user interface.

Accepted: May 17, 2018

Published: June 26, 2018

https://doi.org/10.6028/jres.123.007

1. Summary

Baseline Tailor is an innovative web application for users of the National Institute of Standards and Technology (NIST) Cybersecurity Framework [1] and Special Publication (SP) 800-53 [2]. Baseline Tailor makes the information in these widely referenced publications easily accessible to both security professionals and downstream software by addressing the following barriers:

- Complexity of the rules for tailoring SP 800-53 security controls,
- Differences in the Framework's and SP 800-53 organizational approach,
- Lack of a computer-readable data format for representing tailored security controls.

The NIST Engineering Laboratory’s Cybersecurity for Smart Manufacturing Systems project used Baseline Tailor to help develop a Cybersecurity Framework profile for the manufacturing environment [3]. This “manufacturing profile” uses guidance from NIST SP 800-53 and from NIST SP 800-82 *Guide to Industrial Control Systems Security* [4] to provide manufacturers with a roadmap for reducing cybersecurity risk.

2. Software Specifications

NIST Operating Unit(s)	Engineering Laboratory, Systems Integration Division
Category	Web application for browsing, tailoring, and applying the cybersecurity framework and NIST SP 800-53 control catalogs
Targeted Users	• 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

How to cite this article:
Lubell J (2018) Baseline Tailor.
J Res Natl Inst Stan 123:123007. https://doi.org/10.6028/jres.123.007

	• 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
Operating System(s)	Any. May be run online at https://pages.nist.gov/sctools/bt.xml or installed locally.
Programming Language	XForms 1.1 [5] and Extensible Style Language Transformation (XSLT) 2.0 [6]
Inputs/Outputs	Input is provided and output is displayed using a graphical user interface. Extensible Markup Language (XML) [7] representations of framework profiles and tailored security controls are displayed in multiple-line, resizable text fields.
Documentation	User guide: https://doi.org/10.6028/NIST.IR.8130 Source code: https://github.com/usnistgov/sctools Web page: https://www.nist.gov/services-resources/software/baseline-tailor
Accessibility	N/A
Disclaimer	https://www.nist.gov/director/licensing

3. Implementation

The Baseline Tailor graphical user interface is coded in XForms [5], an XML application for specifying forms for the Web. XForms adopts the model-view-controller software pattern. Baseline Tailor's XForms model [8] consists of a set of instances and a set of bindings. The instances are well-formed XML documents, some static (such as XML representations of the Cybersecurity Framework's core taxonomy and SP 800-53 security controls), and some that change in response to user interaction. The bindings define user interface constraints, compute dynamic instance data values from other instance data, and manage the display of user interface widgets. XForms provides a platform-independent set of widgets, enabling the same XForms-valid source code to run in multiple browser environments and on multiple operating systems.

4. References

[1] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. (Washington, D.C., Department of Commerce), NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.04162018

[2] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Revision 4. https://doi.org/10.6028/NIST.SP.800-53r4

[3] Stouffer K, Zimmerman T, Tang C, Lubell J, Cichonski J, McCarthy J (2017) Cybersecurity Framework Manufacturing Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8183. https://doi.org/10.6028/nist.ir.8183

[4] Stouffer K, Pillitteri V, Lightman S, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Revision 2. https://doi.org/10.6028/NIST.SP.800-82r2

[5] World Wide Web Consortium (2009) *XForms 1.1. W3C Recommendation*. Available at https://www.w3.org/TR/xforms11/

[6] World Wide Web Consortium (2007) *XSL Transformations (XSLT) Version 2.0. W3C Recommendation*. Available at https://www.w3.org/TR/xslt20/

[7] World Wide Web Consortium (2008) *Extensible Markup Language (XML) 1.0 (Fifth Edition). W3C Recommendation*. Available at https://www.w3.org/TR/xml/

[8] Lubell J (2016) Integrating Top-down and Bottom-up Cybersecurity Guidance using XML. *Proceedings of Balisage: The Markup Conference 2016*. https://doi.org/10.4242/BalisageVol17.Lubell01

About the author: *Joshua Lubell is a Computer Scientist in the Systems Integration Division at NIST.*

The National Institute of Standards and Technology is an agency of the U.S. Department of Commerce.