Cybersecurity & Information Systems
Information Analysis Center

CSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

Banking Security Framework

Report Number:
CSIAC-BCO-2022-204
Completed September 2017

CSIAC is a Department of Defense Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443-360-4600

REPORT PREPARED BY:
Philip Payne

Office: CSIAC

Information contained in this report does not constitute endorsement by the U.S. Department of Defense or any nonfederal entity or technology sponsored by a nonfederal entity.

CSIAC is sponsored by the Defense Technical Information Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering. CSIAC is operated by the SURVICE Engineering Company.

DISTRIBUTION A. Approved for public release: distribution unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering, and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
01-09-2017	Technical Research Report	

4. TITLE AND SUBTITLE

Banking Security Framework

5a. CONTRACT NUMBER
FA8075-21-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Philip Payne

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Cybersecurity & Information Systems Information Analysis Center (CSIAC)
SURVICE Engineering Company
4695 Millennium Drive
Belcamp, MD 21017-1505

8. PERFORMING ORGANIZATION REPORT NUMBER

CSIAC-BCO-2022-204

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center (DTIC)
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
Focus areas: cybersecurity

14. ABSTRACT

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) was asked to identify which cybersecurity risk assessment framework is best suited for the financial industry and provide examples of such frameworks. CSIAC identified the National Institute of Standards and Technology Cybersecurity Framework as the most applicable and gave examples of other industry-specific implementation guidance. A presentation specific to the financial services sector was also provided to the inquirer.

15. SUBJECT TERMS
cybersecurity, finance, NIST, CSF, cybersecurity framework

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Ted Welsh, CSIAC Director
U	U	U	UU	8	**19b. TELEPHONE NUMBER** *(include area code)* 443-360-4600

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

DISTRIBUTION A. Approved for public release: distribution unlimited.

ABOUT DTIC AND CSIAC

The Defense Technical Information Center (DTIC) collects, disseminates, and analyzes scientific and technical information to rapidly and reliably deliver knowledge that propels development of the next generation of Warfighter technologies. DTIC amplifies the U.S. Department of Defense's (DoD's) multibillion dollar annual investment in science and technology by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Center's (IAC's) program, which provides critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by, or have access to, hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a DoD IAC sponsored by DTIC to provide expertise in four technical focus areas: cybersecurity; knowledge management & information sharing; modeling & simulation; and software data & analysis. CSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001.

A chief service of the DoD IACs is free technical inquiry (TI) research, limited to 4 research hours per inquiry. This TI response report summarizes the research findings of one such inquiry jointly conducted by CSIAC.

ABSTRACT

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) was asked to identify which cybersecurity risk assessment framework is best suited for the financial industry and provide examples of such frameworks. CSIAC identified the National Institute of Standards and Technology Cybersecurity Framework as the most applicable and gave examples of other industry-specific implementation guidance. A presentation specific to the financial services sector was also provided to the inquirer.

Contents

1.0 TI Request

1.1 INQUIRY

What cyber risk assessment framework best fits the banking sector? How can I find examples?

1.2 DESCRIPTION

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) was asked to identify which cybersecurity risk assessment framework is best suited for the financial industry and provide examples of such frameworks. CSIAC identified the National Institute of Standards and Technology (NIST) Cybersecurity Framework as the most applicable and provided examples of other industry-specific implementation guidance. A presentation specific to the financial services sector was also provided to the inquirer.

2.0 TI Response

From a top-level perspective, the overarching cybersecurity compliance framework for the nation's critical infrastructure (which includes financial services) [1] is NIST's "Framework for Improving Critical Infrastructure Cybersecurity" [2], also referred to as the NIST Cybersecurity Framework (CSF). This publication was released in response to Executive Order (EO) 13636/Presidential Policy Directive (PPD) 21, "Critical Infrastructure Security and Resilience," released in February 2013 [3].

This voluntary cybersecurity risk management strategy consists of three main components:

1. **Framework Core**: a collection of cybersecurity risk management practices and a related hierarchy of functions, categories (e.g., activities and desired outcomes), subcategories, and informative references (e.g., standards defining related security control implementations).
2. **Framework Implementation Tiers**: a scoring system to determine where an organization's cybersecurity policies and practices satisfy components of the NIST CSF. While advancing from lower tiers to higher tiers is recommended, the tiers are not considered to reflect cybersecurity maturity.
3. **Framework Profile**: a profile is determined from an estimation as to where the components of the framework core (i.e., cybersecurity outcomes) rank among the organization's priorities. Profiles can be used to compare an organization's "as is" to the desired "to be" states and facilitate the identification of the necessary improvements to improve that organization's risk posture.

This standardization is an important step towards implementing a unified framework instead of industry-specific (or ad-hoc) solutions that fail to provide a comprehensive strategy. However, it also presents the challenge of having to address such a wide range of critical infrastructure sectors. As such, the guidance is typically written at a higher-level so the individual sectors can develop and publish industry-specific implementation guidance consistent with the higher-level NIST CSF. For example, the Department of Energy has published documentation for the energy sector, including "Energy Sector Cybersecurity Framework Implementation Guidance" [4] and the "Cybersecurity Capability Maturity Model (C2M2)" [5]. CSIAC is not currently aware of a similar implementation guide for the banking/finance sector but admittedly is funded to support the defense community.

Information security has been, and continues to remain, a critical requirement for the banking sector given the obvious motivation for attacks and the severity of the potential consequences. As such, a variety of industry-specific frameworks has been developed for this community. Furthermore, the many different components of the financial services sector and the related regulatory bodies have further convoluted the cybersecurity requirements and compliance reporting. Research suggests that similar standardization efforts are underway to address this issue, which are likely best described by the accompanying NIST presentation "Financial Services Sector Specific Cybersecurity "Profile," an NIST cybersecurity workshop in coordination with the Financial Services Sector Coordinating Council [6].

REFERENCES

[1] Cybersecurity & Infrastructure Security Agency. "Critical Infrastructure Sectors." https://www.dhs.gov/critical-infrastructure-sectors, 21 October 2020.

[2] NIST. "Framework for Improving Critical Infrastructure Cybersecurity." Draft version 1.1, https://www.nist.gov/cyberframework, January 2017.

[3] The White House. Presidential Policy Directive (PPD) 21. "Critical Infrastructure Security and Resilience," 12 February 2013.

[4] Office of Cybersecurity, Energy Security, and Emergency Response. "Energy Sector Cybersecurity Framework Implementation Guidance," 6 January 2015.

[5] Office of Cybersecurity, Energy Security, and Emergency Response. "Cybersecurity Capability Maturity Model (C2M2)." https://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity, July 2021.

[6] Financial Services Sector Coordinating Council. "Financial Services Sector Specific Cybersecurity 'Profile'." NIST Cybersecurity Workshop, 17 May 2017.