NIST SPECIAL PUBLICATION 1800-39A

Implementing Data Classification Practices

Volume A:
Executive Summary

William Newhouse
Murugiah Souppaya
National Institute of Standards and Technology
Gaithersburg, Maryland

John Kent
Ken Sandlin
The MITRE Corporation
McLean, Virginia

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

April 2023

PRELIMINARY DRAFT

This draft was updated on May 2, 2023

This publication is available free of charge from
https://www.nccoe.nist.gov/data-classification

Executive Summary

Organizations are managing an increasing volume of data while maintaining compliance with policies for protecting that data. Those policies are driven by business, regulatory, data security, and privacy requirements. This publication can help organizations reduce the risk of data breaches, loss, and mishandling through data-centric security management by demonstrating how to discover and classify data based on its characteristics regardless of where the data resides or how it is shared. As part of a zero-trust approach, security management depends on organizations knowing what data they have, what the data's characteristics are, and the organization's security and privacy requirements for that data. The example solutions in this guide focus on using data classification in various use cases to inform the protection of data that is used by an organization and shared between organizations. The guide's use cases will demonstrate commercially available products that enable data classification. The first use case focuses on classifying data used in email messages exchanged within and between organizations.

This 1800-series National Institute of Standards and Technology (NIST) publication documents how the National Cybersecurity Center of Excellence (NCCoE) and its collaborators are using commercially available technology to build interoperable data classification solutions for use cases. As the project progresses, this preliminary draft will be updated with supporting guidance, and additional use cases and volumes will also be released to solicit public comment.

CHALLENGE

Significant challenges that have hindered effective use of data classification for protecting data include:

- The limited nature of actionable and interoperable standards for data classification across different regulated industry sectors means that many organizations do not use classifications that are consistent with those of their partners and suppliers to support various policies.
- The lack of shared data classification schemes can result in data being classified and labeled inconsistently.
- Data being widely distributed across data centers, clouds, and endpoint devices complicates the process of establishing and maintaining data inventories.
- Data classifications and data handling requirements often change during the data lifecycle, requiring the capability to adjust to those changing requirements.
- Organizational culture may not connect its data owners and business process owners with its data classification technology operators.

This practice guide can help your organization:

- Adopt, support, and implement interoperable data classification schemas
- Mitigate the security and privacy risks of sharing data within and among organizations
- Become familiar with commercially available solutions that can help classify data
- Develop and strengthen a common language for data classification

SOLUTION

The NCCoE is collaborating with technology providers to build several example data classification solutions and demonstrate their ability to meet organizational data classification needs. The project's objective is to define product-agnostic recommended practices for defining data classification schemes and communicating them to others. Organizations will also be able to use the recommended practices to inventory and characterize data for other security management purposes, such as prioritization of data in preparing the migration of systems, applications, and services to support post-quantum cryptographic algorithms.

For the first example solution, the use case involves the creation, transmission, storage, and retrieval of email. The solution focuses on the classification and exchange of email messages and attachments within and among multiple organizations. Additional volumes of this publication will be released in the future. Volumes will document how organizations can apply zero-trust-aligned approaches to solve the challenge of exchanging data via email using data classification techniques. Future volumes will include data classification guidance, example solution architectures, demonstrations of the technology, and mapping relationships to support various government and industry-recommended practices.

Our solution strategy follows an agile implementation methodology to build iteratively and incrementally while adapting or adding capabilities. Additional data classification use cases will be examined to address an increasing number of requirements and resource types.

The following collaborators are working with NIST on this project.

Collaborators		
ActiveNav	Janusnet	Thales Trusted Cyber Technologies
Adobe	JPMorgan Chase & Co.	Trellix
GitLab	Quick Heal	Virtru
Google		

While the NCCoE is using a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security, business security officers, and technology officers can use this part of the guide, *NIST SP 1800-39a: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Future releases of this publication will include guidance to assist people in the following roles:

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk will be able to use *NIST SP 1800-39b: Approach, Architecture, and Security Characteristics,* which will describe what we built and why, including the risk analysis performed and the security/privacy control mappings once it is published.

IT professionals who want to implement an approach like this will be able to make use of *NIST SP 1800-39c: How-To Guides*, which will provide specific product installation, configuration, and integration instructions for building the example implementations, allowing you to replicate all or parts of this project once it is published.

SHARE YOUR FEEDBACK

Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments, contact the NCCoE at data-nccoe@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.