# MITM-ing cryptographic standards

Looking back on a 3 year old accident How the f\*\*\* did we get there again?

Tales from a Rogue Archive

# MITM-ing cryptographic standards

Looking back on a 3 year old accident How the f\*\*\* did we get there again?

Tales from a Rogue Archive

\*not sponsored by



MITM-ing cryptographic standards

Looking back on a 3 year old accident How the f\*\*\* did we get there again?

Tales from a Rogue Archive







\*not sponsored by





**Projects** 

75

**Publications** +

+ **Topics** 

**News & Updates** 

**Events** 

Glossary

+ About CSRC

# POPULAR LINKS 4

**Crypto Standards & Guidelines** 

**Publications:** 

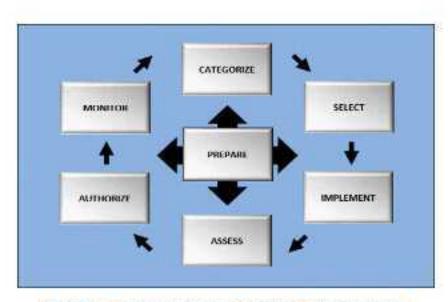
Drafts / FIPS / SP 800s

**Crypto Module Validation** 

FIPS 140-2 Modules & Vendors

**Crypto Algorithm Validations** 

**Risk Management Framework** 



NIST UPDATES THE RISK MANAGEMENT FRAMEWORK (SP 800-37 REV. 2)!



**NEW SEARCH INTERFACE AVAILABLE FOR** CRYPTO ALGORITHM VALIDATIONS



REQUESTING LIGHTWEIGHT CRYPTO **ALGORITHM NOMINATIONS** 

For 20 years, the Computer Security Resource Center (CSRC) has provided access to NIST's cybersecurity- and information security-related projects, publications, news and events. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- · see our greatly-expanded publications library,
- · explore content by topic,
- · search our glossary of information security terms, and
- subscribe to CSRC email updates.

# RECENT NEWS

#### RMF Update: NIST Publishes SP 800-37 Rev. 2

December 20, 2018

NIST has published an update to its Risk Management Framework specification, in NIST Special Publication (SP) 800-37 Revision 2.

# NIST Releases Draft SP 800-189 for Comment

December 17, 2018

Draft Special Publication 800-189, "Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation," is now available for comment. The deadline for submitting comments is February 15, 2019.

#### NIST Publishes NISTIR 8011 Vol. 3



**Projects** 

Publications +

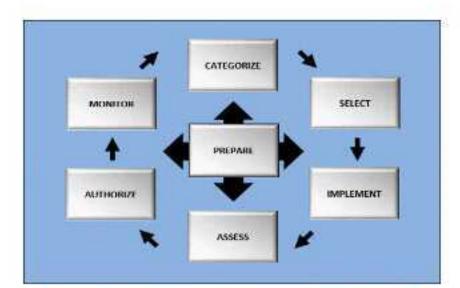
Topics +

**News & Updates** 

**Events** 

Glossary

About CSRC +



FRAMEWORK (SP 800-37 REV. 2)!



NEW SEARCH INTERFACE AVAILABLE FOR CRYPTO ALGORITHM VALIDATIONS



REQUESTING LIGHTWEIGHT CRYPTO
ALGORITHM NOMINATIONS

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded publications library,
- explore content by topic,
- · search our glossary of information security terms, and
- subscribe to CSRC email updates.

# POPULAR LINKS 4

Crypto Standards & Guidelines

Publications:

Drafts / FIPS / SP 800s

Crypto Module Validation

FIPS 140-2 Modules & Vendors

**Crypto Algorithm Validations** 

**Risk Management Framework** 

# RECENT NEWS

#### RMF Update: NIST Publishes SP 800-37 Rev. 2

December 20, 2018

NIST has published an update to its Risk Management Framework specification, in NIST Special Publication (SP) 800-37 Revision 2.

# NIST Releases Draft SP 800-189 for Comment

December 17, 2018

Draft Special Publication 800-189, "Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation," is now available for comment. The deadline for submitting comments is February 15, 2019.

#### NIST Publishes NISTIR 8011 Vol. 3



Search CSRC Q

PROJECTS

# **Cryptographic Standards and Guidelines**



# **Project Overview**

Users of the former "Crypto Toolkit" can now find that content under this project. It includes cryptographic primitives, algorithms and schemes are described in some of NIST's Federal Information Processing Standards (FIPS), Special Publications (SPs) and NIST Internal/Interagency Reports (NISTIRs).

# Crypto Standards and Guidelines, by Project Area

- Block Cipher Techniques
- Digital Signatures
- Hash Functions
- Key Management
- Message Authentication Codes (MACs)
- Post-quantum Techniques
- Random Bit Generation

# Implementation-related References

- Examples with Intermediate Values
- Object Identifiers (OIDs): Computer Security Objects Register
- Cryptographic Algorithm Validation Program (CAVP)



#### Overview

#### **Publications**

# ADDITIONAL PAGES

#### **Example Values**

**Crypto-Enabled Applications** 

**Withdrawn Crypto Standards** 

**Archived Crypto Projects** 

**AES Development** 



#### Dr. Lily Chen

lily.chen@nist.gov

# ♣ GROUP

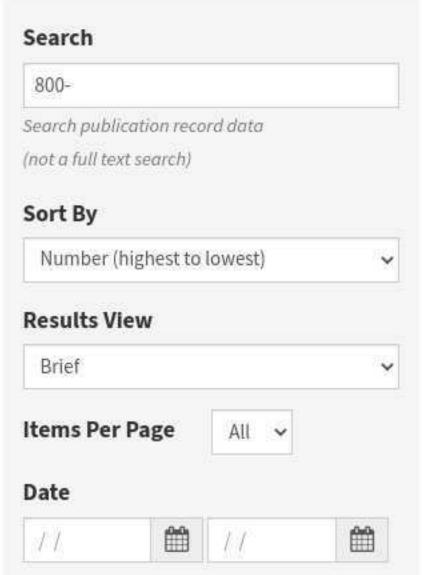
Cryptographic Technology

# **RELATED PROJECTS**



# **Publication Search**





# Search Results

Keywords: ×800- Sorted By: × Number (highest to lowest) Status: × Draft × Final Series: × SP
Showing 170 matching records.

Series	Number	Title	Status	Release Date
SP	800-203	2017 NIST/ITL Cybersecurity Program Annual Report Download: SP 800-203 (DOI); Local Download	Final	7/02/2018
SP	800-202	Quick Start Guide for Populating Mobile Test Devices  Download: SP 800-202 (DOI); Local Download; Computer Forensics Tool Testing (CFTT) Program;  CFTT Federated Testing Project	Final	5/10/2018
SP	800-195	2016 NIST/ITL Cybersecurity Program Annual Report  Download: SP 800-195 (DOI); Local Download	Final	9/28/2017
SP	800-193	Platform Firmware Resiliency Guidelines  Download: SP 800-193 (DOI); Local Download	Final	5/04/2018
SP	800-192	Verification and Test Methods for Access Control Policies/Models  Download: SP 800-192 (DOI); Local Download	Final	6/27/2017
SP	800-190	Application Container Security Guide  Download: SP 800-190 (DOI); Local Download	Final	9/25/2017
SP	800-189	Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation Download: SP 800-189 (DRAFT) (DOI); Local Download	Draft	12/17/2018
SP	800-188	De-Identifying Government Datasets (2nd Draft)  Download: Draft SP 800-188; Comment Template	Draft	12/15/2016
SP	800-187	Guide to LTE Security  Download: SP 800-187 (DOI); Local Download	Final	12/21/2017
SP	800-185	SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash  Download: SP 800-185 (DOI); Local Download; Comments Received on Draft SP 800-185	Final	12/22/2016

Information Technology Laboratory

# COMPUTER SECURITY RESOURCE CENTER



**PROJECTS** 

CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

# **Cryptographic Module Validation Program**



# Validated Modules

All questions regarding the implementation and/or use of any validated cryptographic module should first be directed to the appropriate VENDOR point of contact (listed for each entry).

#### SEARCH our database of validated modules.

The FIPS 140-1 and FIPS 140-2 validated modules search provides access to the official validation information of all cryptographic modules that have been tested and validated under the Cryptographic Module Validation Program as meeting requirements for FIPS PUB 140-1 and FIPS PUB 140-2. The search results list all issued validation certificates that meet the supplied search criteria and provide a link to view more detailed information about each certificate. The Certificate Detail listing provides the detailed module information including algorithm implementation references to the CAVP algorithm validation, Security Policies, original certificate images or reference to the consolidated validation lists, and vendor product links if provided.

If a validation certificate is marked as **revoked**, the module validation is no longer valid and may not be referenced to demonstrate compliance to FIPS 140-1 or FIPS 140-2.

If a validation certificate is marked as **historical**, Federal Agencies should not include these in new procurement. This does not mean that the overall FIPS-140 certificates for these modules have been revoked, rather it indicates that the certificates and the documentation posted with them are more than 5 years old and have not been updated to reflect latest guidance and/or transitions, and may not accurately reflect how the module can be used in FIPS mode. Agencies may make a risk determination on whether to continue using the modules on this list based on their own assessment of where and how the module is used.

It is important to note that validation certificates are issued for cryptographic modules. A module may either be an

# % PROJECT LINKS

#### Overview

#### News

# ADDITIONAL PAGES

#### Standards

#### IG Announcements

Announcements Archive

#### Contacts

#### Notices

#### Validated Modules

#### Search

#### Modules In Process

Modules In Process List

Implementation Under Test List

**CMVP Management Manual and FAOs** 

Use of FIPS 140-2 Logo and Phrases

# CONTACTS

# Beverly Trapnell

**NIST CMVP Acting Program Manager** 

cmvn@nist gov



Information Technology Laboratory

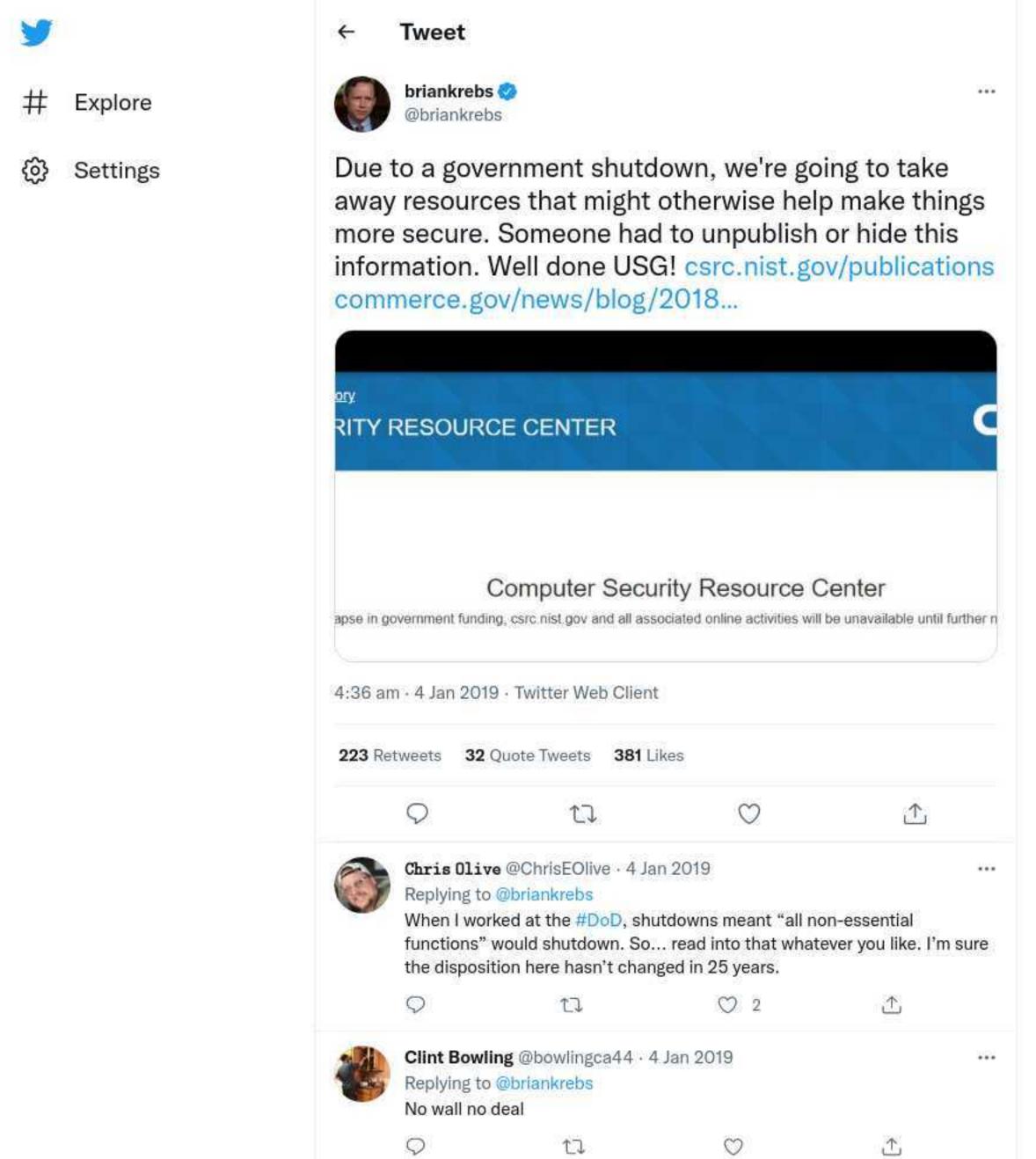
# COMPUTER SECURITY RESOURCE CENTER

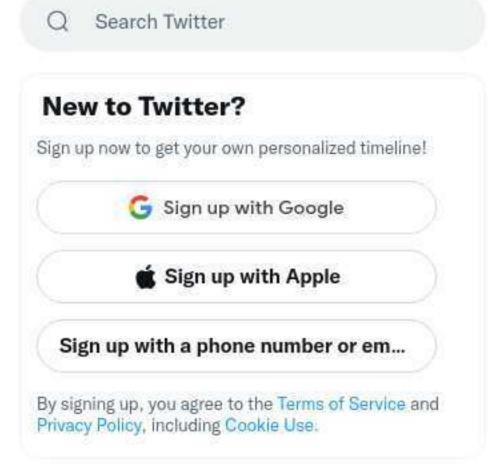


# Computer Security Resource Center

Due to the lapse in government funding, csrc.nist.gov and all associated online activities will be unavailable until further notice. Learn more.

A



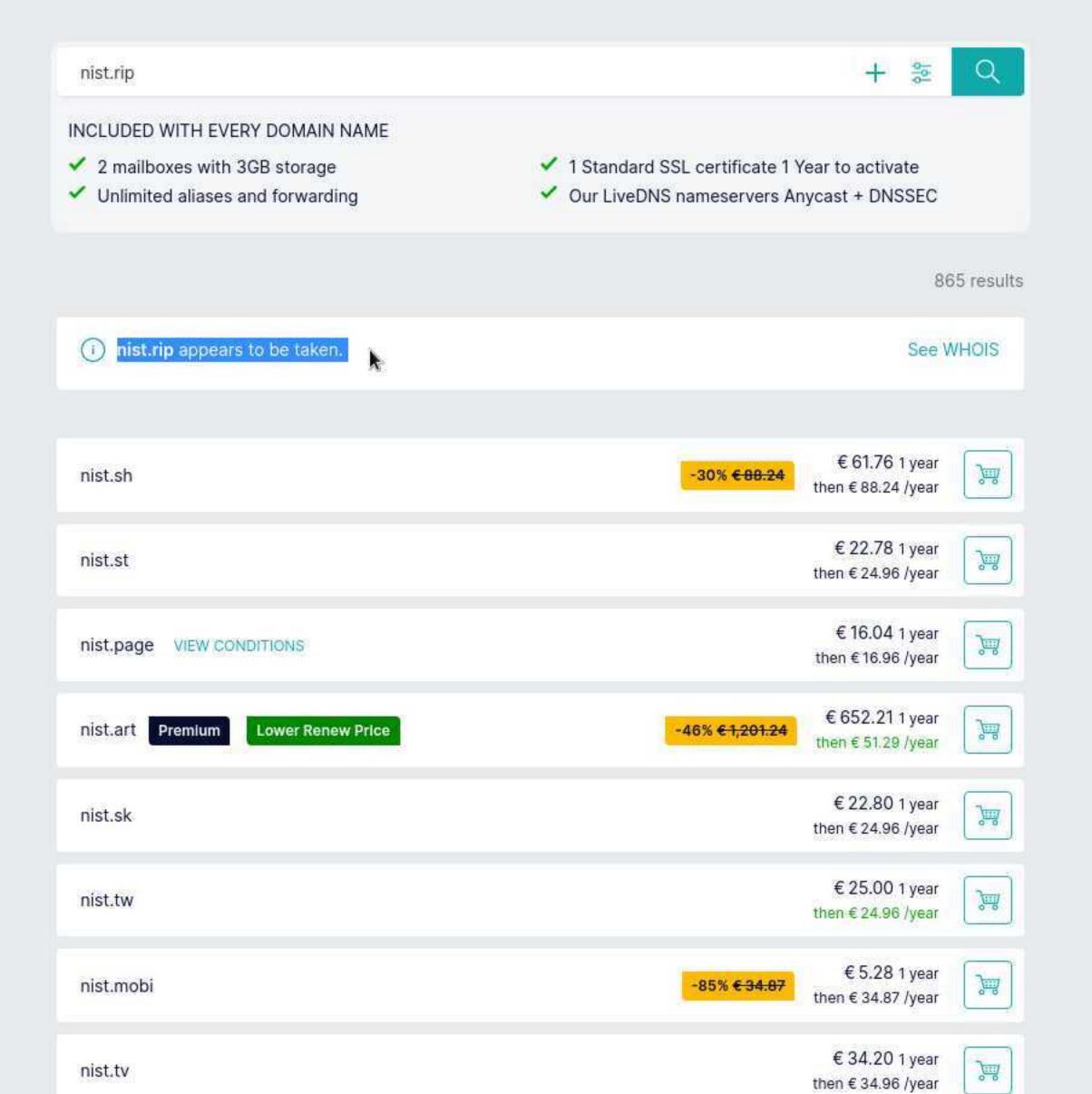




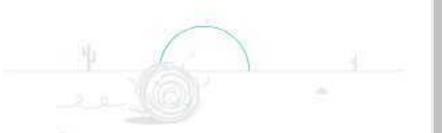




# Register a domain name



# Shopping Cart o



## Your shopping cart is empty

Looks like you haven't added anything to your cart yet

Prices for France, incl. VAT in € (EUR) Change



Chat with us



**Projects** 

Publications +

Topics +

**News & Updates** 

**Events** 

Glossary

About CSRC +



# POPULAR LINKS 4

**Crypto Standards & Guidelines** 

#### **Publications:**

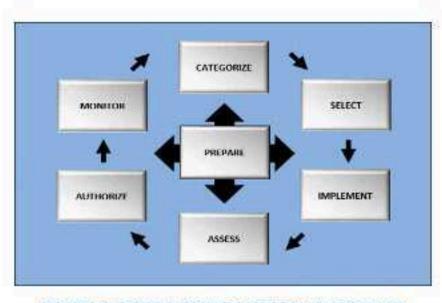
Drafts / FIPS / SP 800s

**Crypto Module Validation** 

FIPS 140-2 Modules & Vendors

**Crypto Algorithm Validations** 

**Risk Management Framework** 



FRAMEWORK (SP 800-37 REV. 2)!



NEW SEARCH INTERFACE AVAILABLE FOR CRYPTO ALGORITHM VALIDATIONS



REQUESTING LIGHTWEIGHT CRYPTO
ALGORITHM NOMINATIONS

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded publications library,
- explore content by topic,
- search our glossary of information security terms, and
- subscribe to CSRC email updates.

# RECENT NEWS

#### RMF Update: NIST Publishes SP 800-37 Rev. 2

#### December 20, 2018

NIST has published an update to its Risk Management Framework specification, in NIST Special Publication (SP) 800-37 Revision 2.

# NIST Releases Draft SP 800-189 for Comment

#### December 17, 2018

Draft Special Publication 800-189, "Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation," is now available for comment. The deadline for submitting comments is February 15, 2019.

#### NIST Publishes NISTIR 8011 Vol. 3



**Projects** 

Publications +

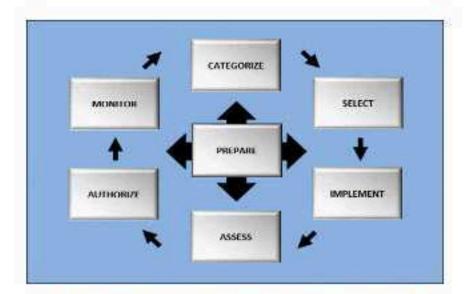
Topics +

**News & Updates** 

**Events** 

Glossary

About CSRC +



FRAMEWORK (SP 800-37 REV. 2)!



NEW SEARCH INTERFACE AVAILABLE FOR CRYPTO ALGORITHM VALIDATIONS

For 20 years, the Computer Security Resource Center (CSRC) has provided access to NIST's cybersecurity- and information security-related



REQUESTING LIGHTWEIGHT CRYPTO
ALGORITHM NOMINATIONS

# POPULAR LINKS 5

**Crypto Standards & Guidelines** 

#### **Publications:**

Drafts / FIPS / SP 800s

**Crypto Module Validation** 

FIPS 140-2 Modules & Vendors

**Crypto Algorithm Validations** 

**Risk Management Framework** 

projects, publications, news and events. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded publications library,
- explore content by topic,
- search our glossary of information security terms, and
- subscribe to CSRC email updates.

# RECENT NEWS

## RMF Update: NIST Publishes SP 800-37 Rev. 2

#### December 20, 2018

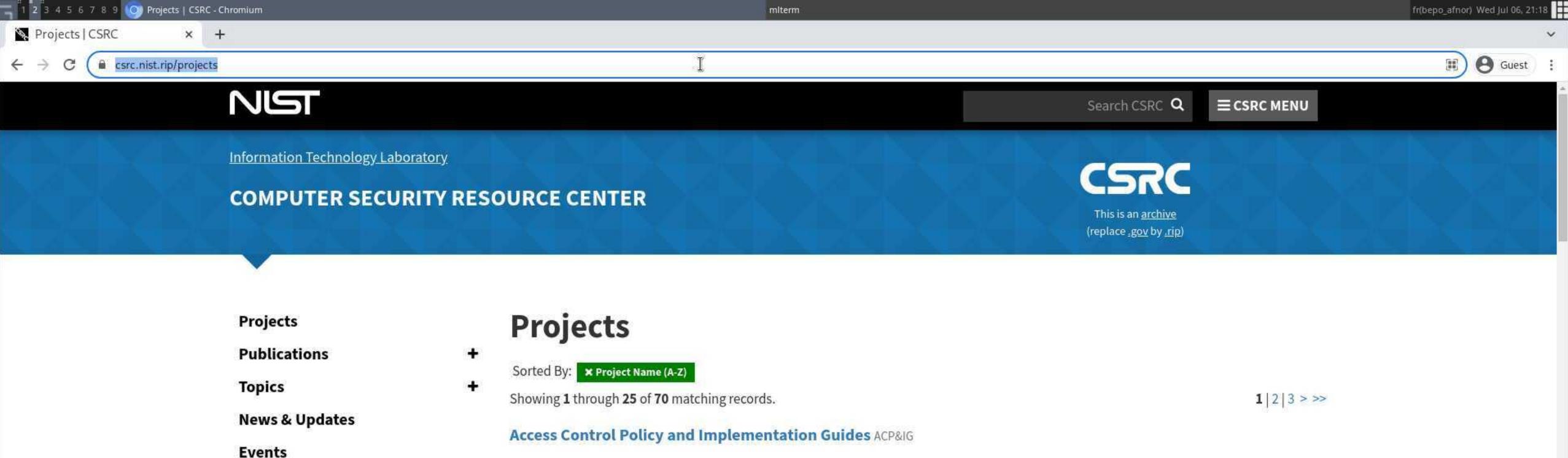
NIST has published an update to its Risk Management Framework specification, in NIST Special Publication (SP) 800-37 Revision 2.

# NIST Releases Draft SP 800-189 for Comment

#### December 17, 2018

Draft Special Publication 800-189, "Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation," is now available for comment. The deadline for submitting comments is February 15, 2019.

#### NIST Publishes NISTIR 8011 Vol. 3



Adequate security of information and information systems is a fundamental management responsibility. Nearly all applications that deal with financial, privacy, safety, or defense include some form of access (authorization) control. Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system. In some systems, complete access is granted after s successful authentication of the user, but most...

## Access Control Policy Testing ACPT

Glossary

Search

Sort By

Topics

About CSRC

Search Project Name, Acronym, Description

Relevance (best match)

Match ANY: 

Match ALL:

**Items Per Page** 

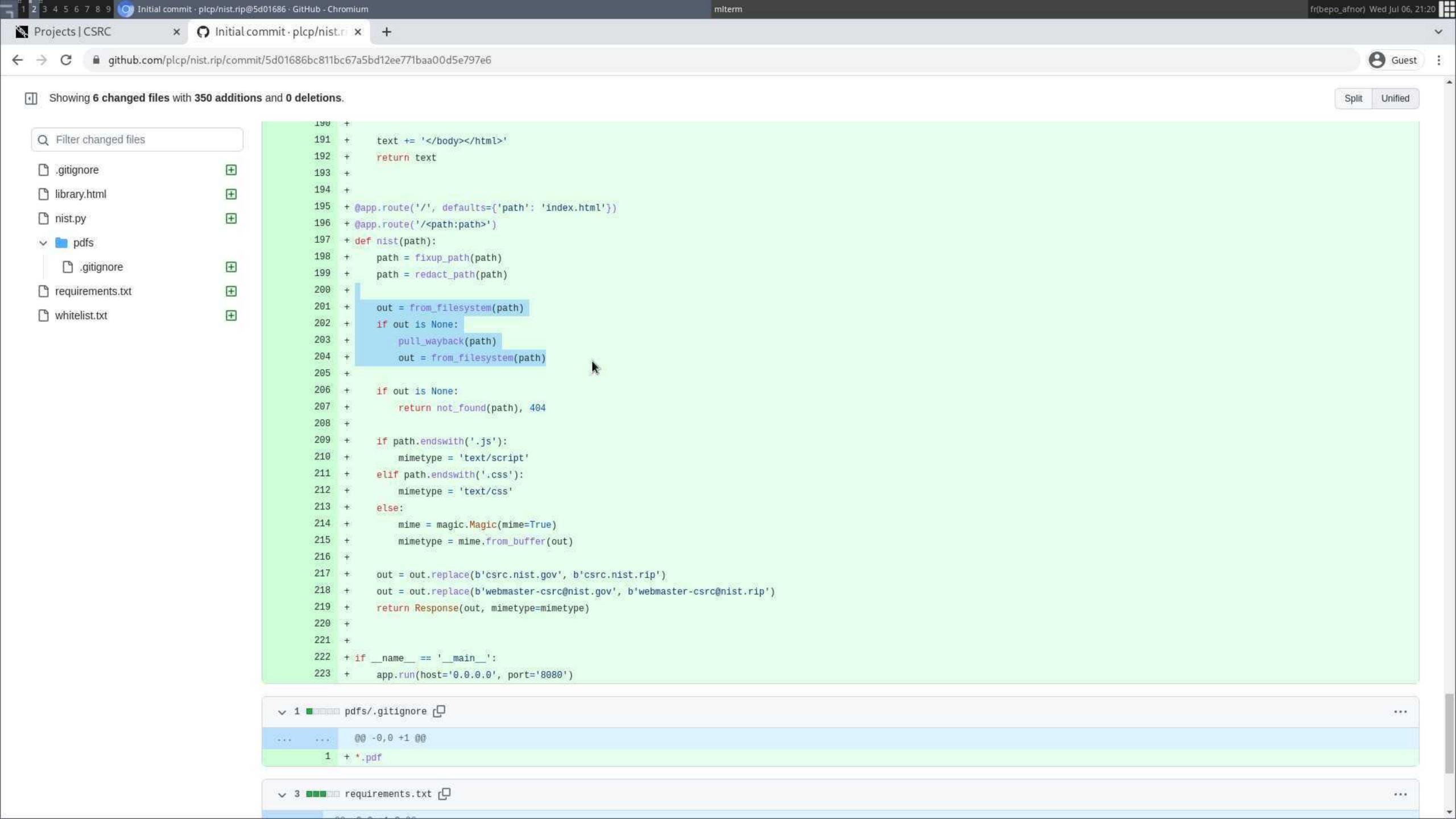
Access control systems are among the most critical security components. Faulty policies, misconfigurations, or flaws in software implementation can result in serious vulnerabilities. The specification of access control policies is often a challenging problem. Often a system's privacy and security are compromised due to the misconfiguration of access control policies instead of the failure of cryptographic primitives or protocols. This problem becomes increasingly severe as software systems...

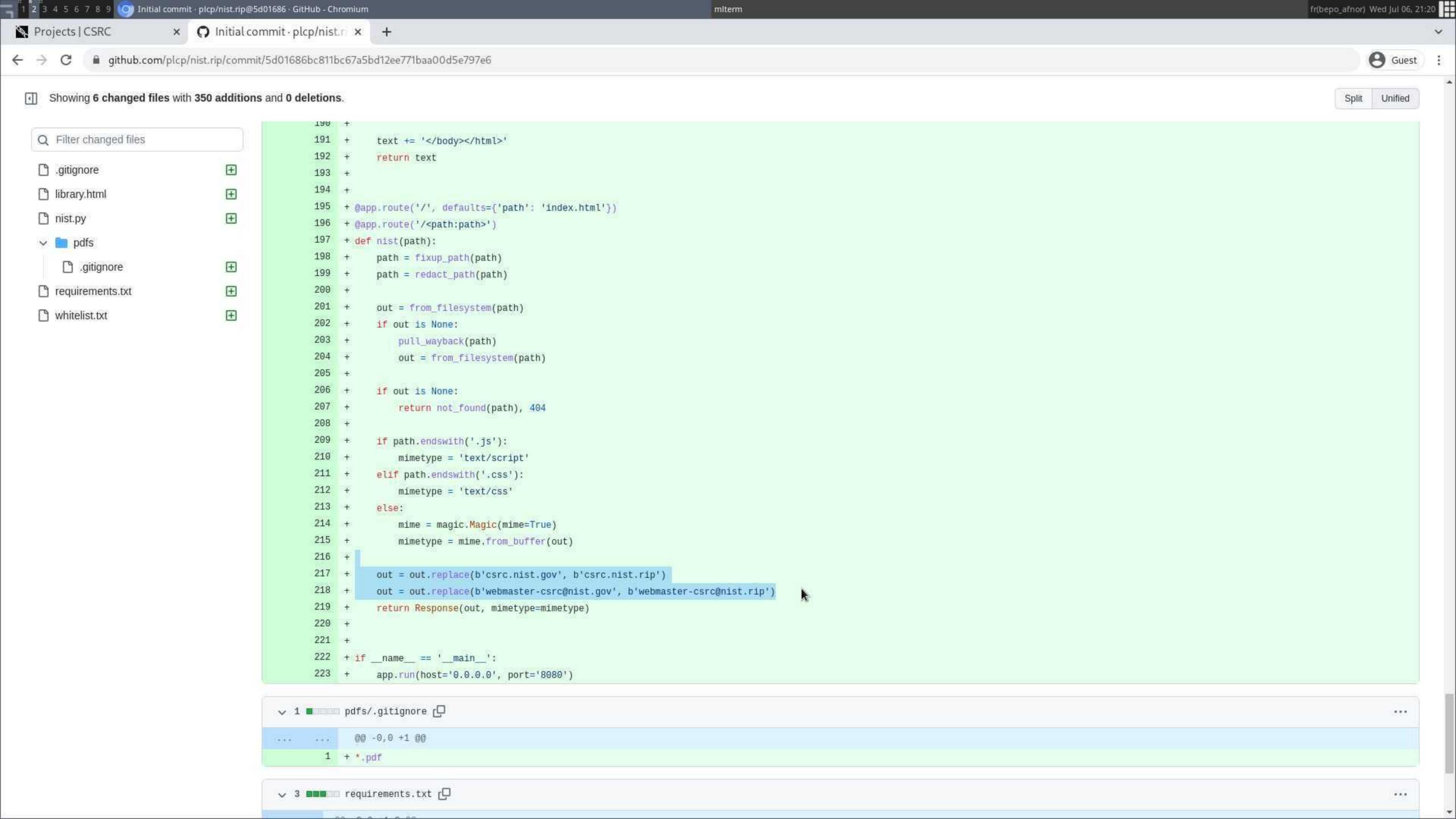
# Algorithms for Intrusion Measurement AIM

The Algorithms for Intrusion Measurement (AIM) project furthers measurement science in the area of algorithms used in the field of intrusion detection. The team focuses on both new detection metrics and measurements of scalability (more formally algorithmic complexity). This analysis is applied to different phases of the detection lifecycle to include pre-emptive vulnerability analysis, initial attack detection, alert impact, alert aggregation/correlation, and compact log storage. In...

# Apple macOS Security Configuration APPLE-OS

CSD's macOS security configuration team is working to develop secure system configuration baselines supporting different operational















# **Recommendation for Random Number Generation Using Deterministic Random Bit Generators**

Elaine Barker John Kelsey

This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1

COMPUTER SECURITY



v X

98

99



100



101



102



NIST SP 800-90A Rev. 1

Recommendation for Random Number Generation Using Deterministic RBGs

### Appendix D: (Informative) References

- [FIPS 140] Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 25, 2001 (including Change Notices as of December 3, 2002). http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [accessed 6/9/15].
- [FIPS 180] Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard (SHS), March 2012. http://csrc.nist.rip/publications/fips/fips180-4/fips-180-4.pdf [accessed 6/9/15].
- Federal Information Processing Standard (FIPS) 197, Advanced Encryption [FIPS 197] Standard (AES), November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [accessed 6/9/15].
- Federal Information Processing Standard (FIPS) 198-1, The Keyed-Hash Message [FIPS 198] Authentication Code (HMAC), July 2008. http://csrc.nist.rip/publications/fips/fips198 -1/FIPS-198-1 final.pdf [accessed 6/9/15].
- [SP 800-38A] National Institute of Standards and Technology Special Publication (SP) 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001. http://csrc.nist.rip/publications/nistpubs/800-38a/sp800-38a.pdf [accessed] 6/9/15].
- [SP 800-38D] National Institute of Standards and Technology Special Publication (SP) 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007. http://csrc.nist.rip/publications/nistpubs/800-38D/SP-800-38D.pdf [accessed] 6/9/15].
- NIST Special Publication (SP) 800-57 Part 1 Revision 3, Recommendation for Key Management-Part 1: General, July 2012. http://csrc.nist.rip/publications/nistpubs/800-57/sp800 -57 part1 rev3 general.pdf [accessed 6/9/15].
- NIST Special Publication (SP) 800-67 Revision 1, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, January 2012. http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf [accessed
- [SP 800-90B] NIST Special Publication (SP) 800-90B (Draft), Recommendation for the Entropy Sources Used for Random Bit Generation, August 2012 [re-released September http://csrc.nist.rip/publications/drafts/800-90/draft-sp800-90b.pdf [accessed 6/9/15].
- [SP 800-90C] NIST Special Publication (SP) 800-90C (Draft), Recommendation for Random Bit Generator (RBG) Constructions, August 2012 [re-released September 2013].







5





7

however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-90A Revision 1 Natl. Inst. Stand. Technol. Spec. Publ. 800-90A Rev. 1, 109 pages (June 2015) CODEN: NSPUE2

> This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

#### Comments may be provided to:

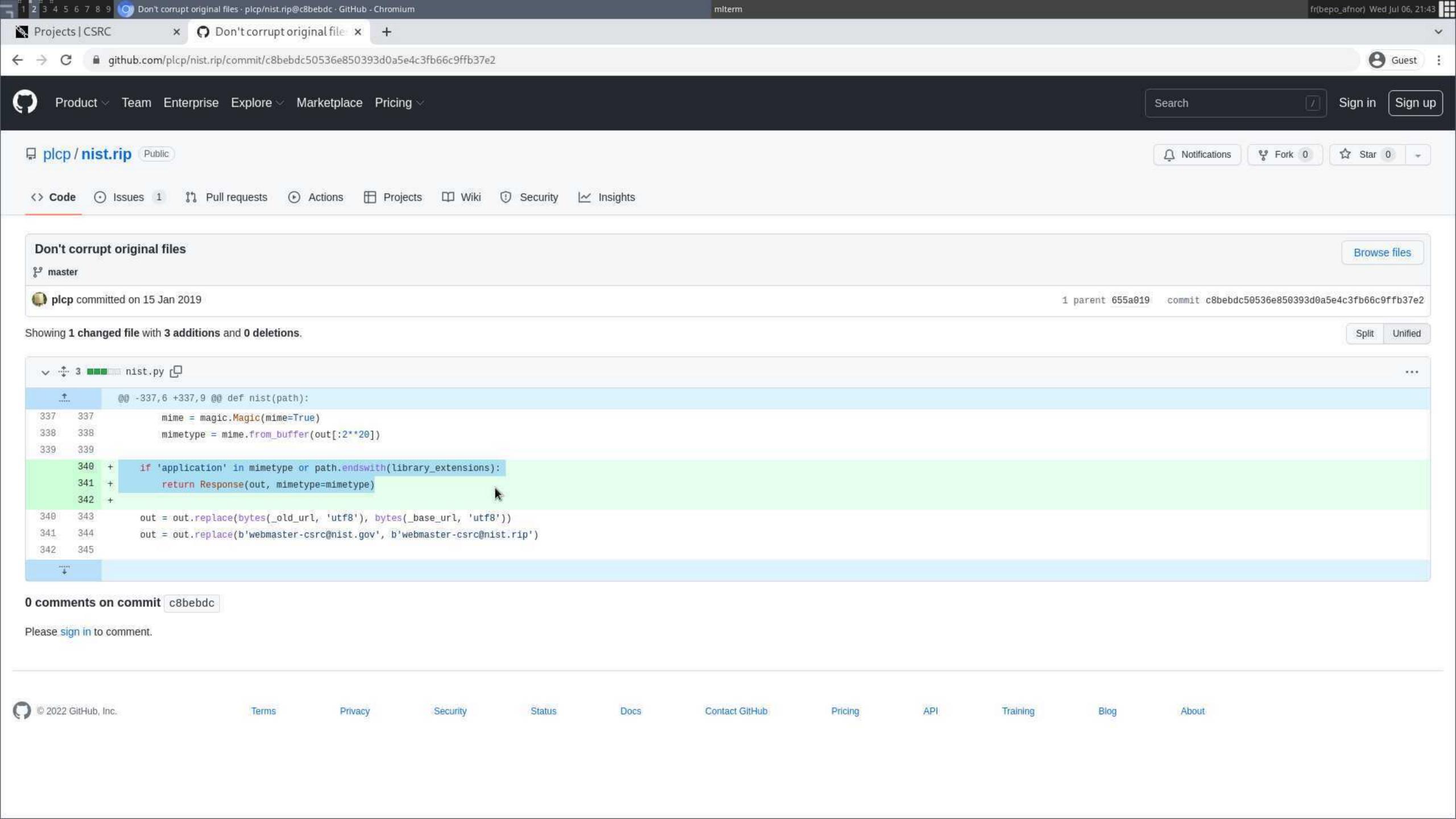
National Institute of Standards and Technology Attn: Computer Security Division, Information Technology Laboratory 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930 Email: rbg\_comments@nist.rip

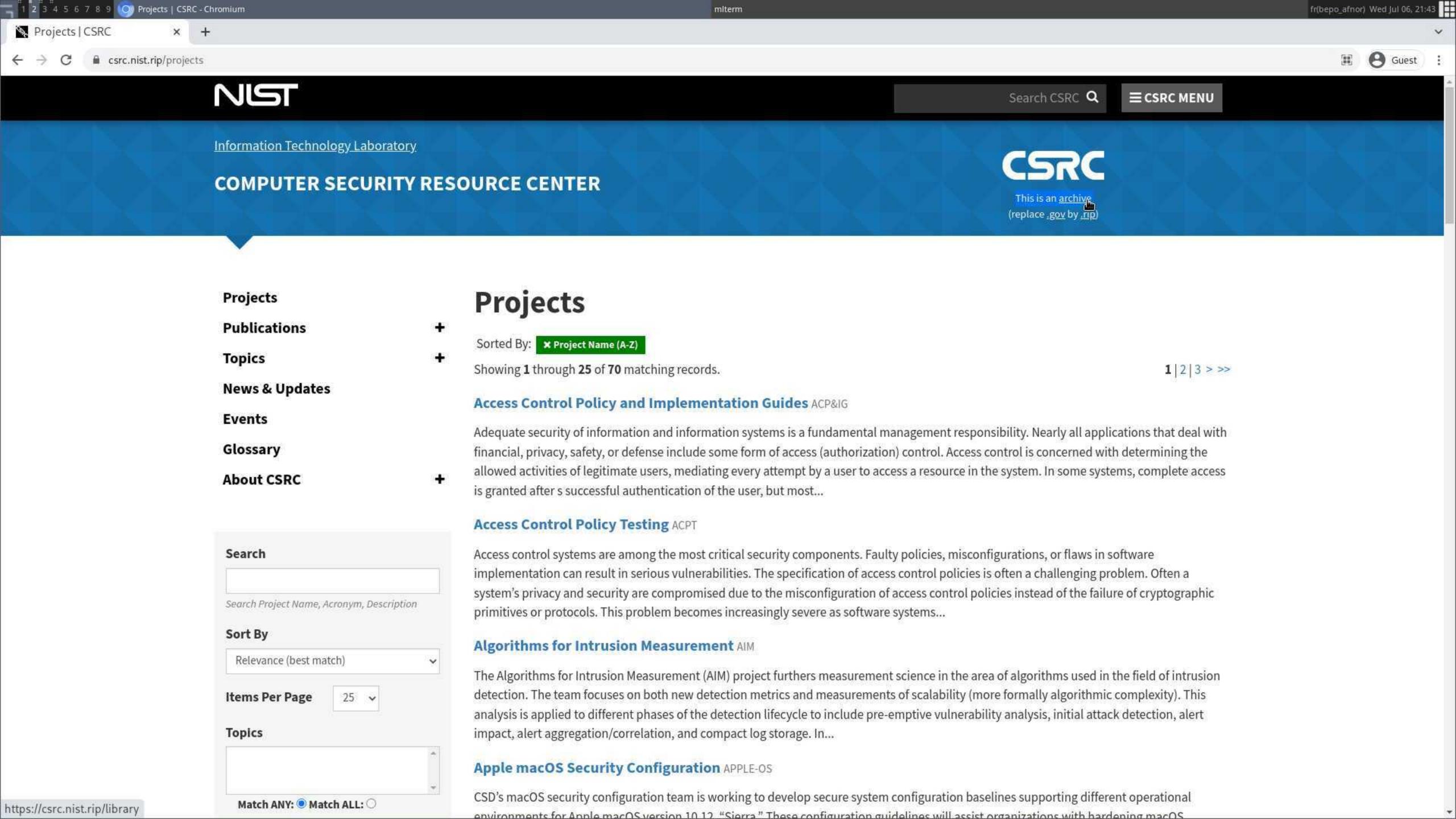
NIST SP 800-90A Rev. 1

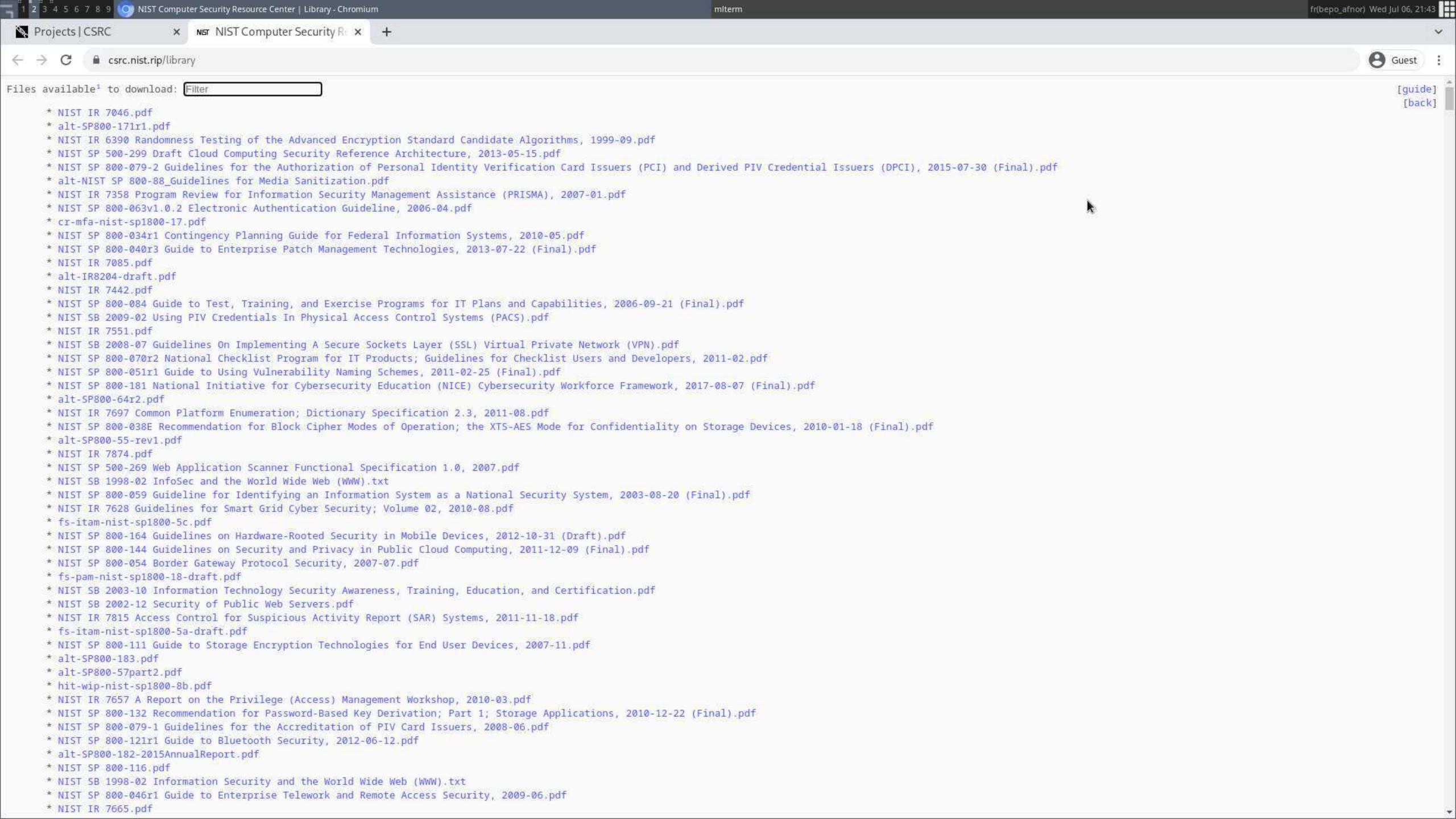
Recommendation for Random Number Generation Using Deterministic RBGs

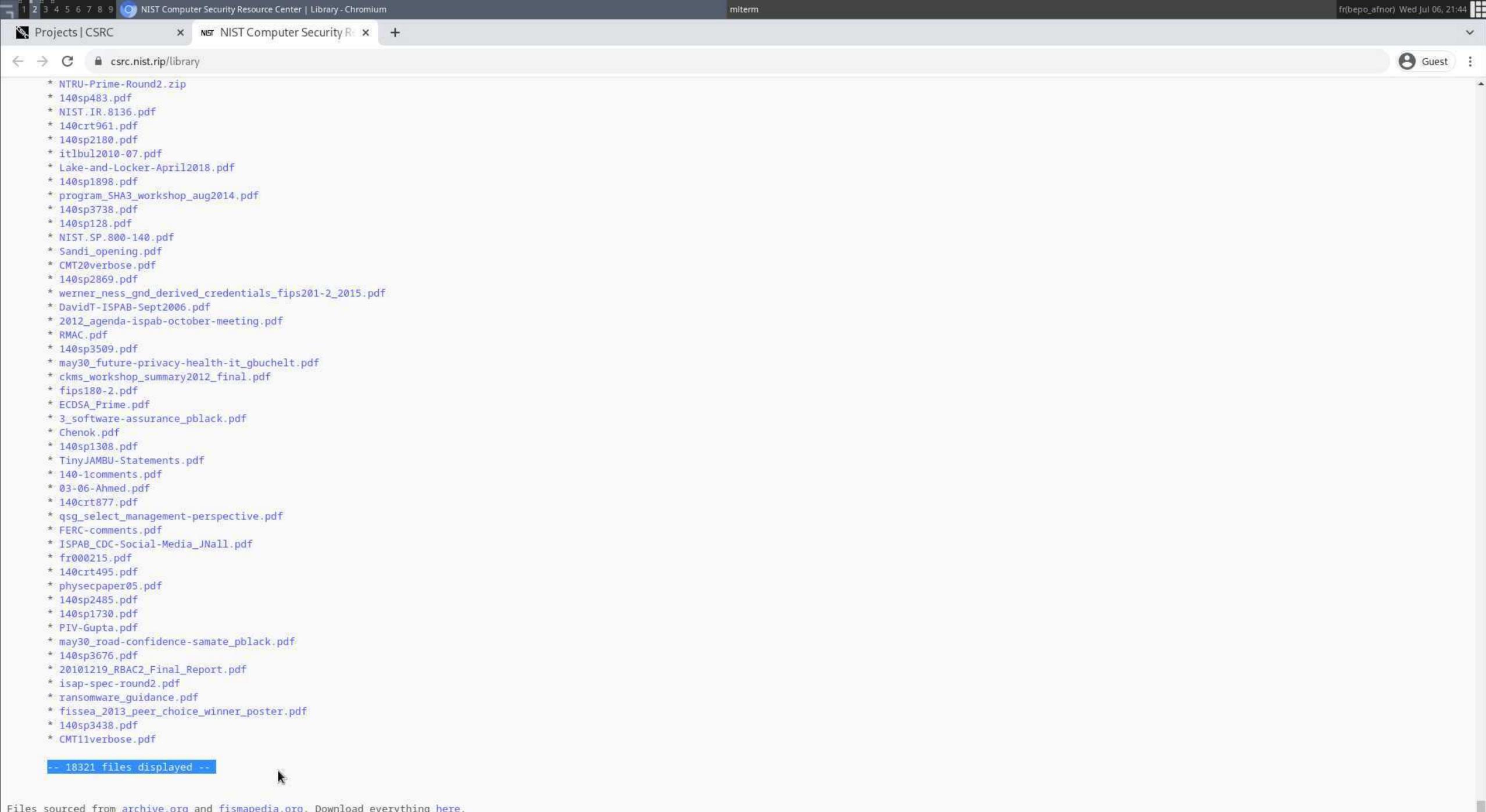
# Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.







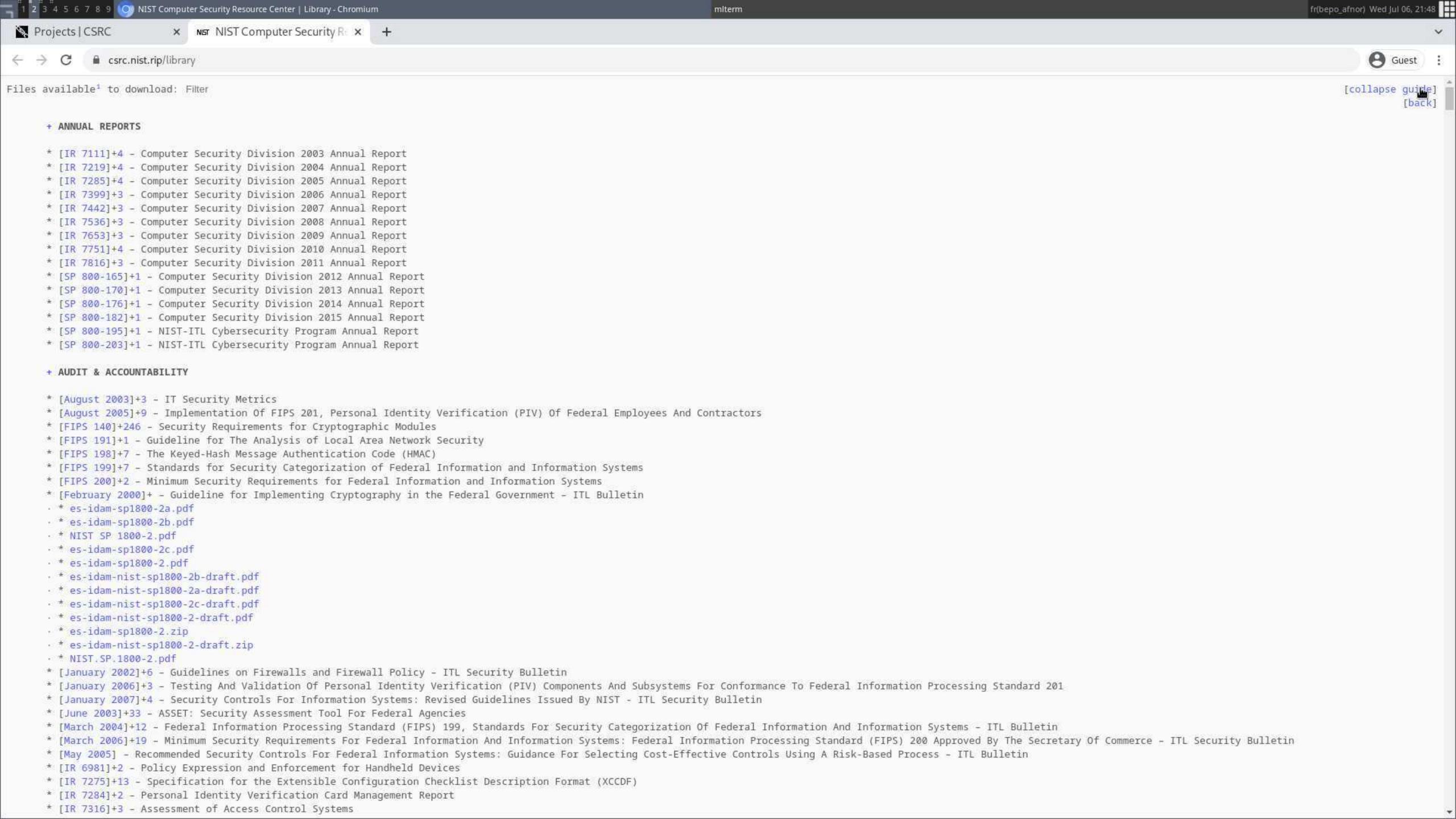


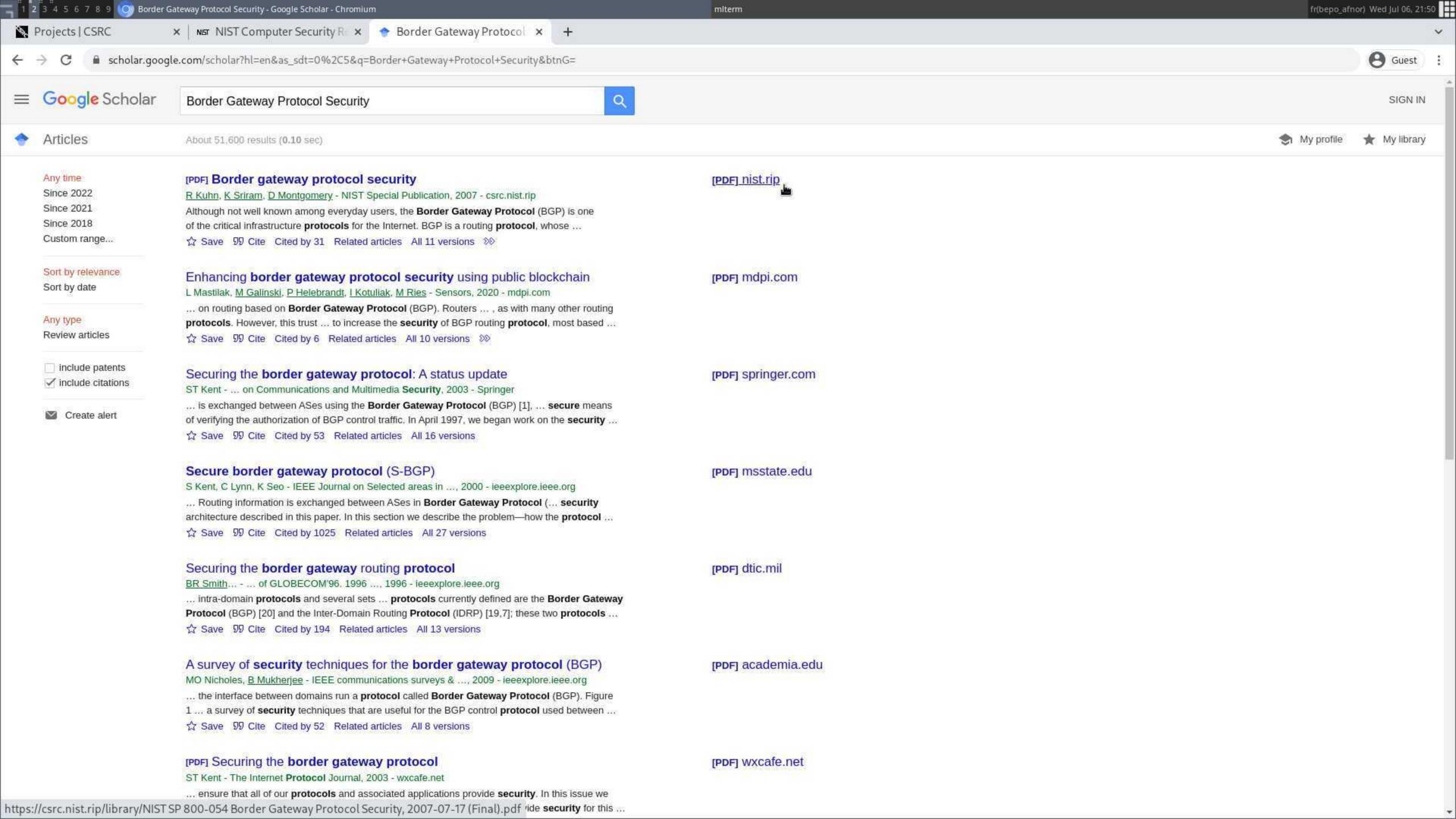


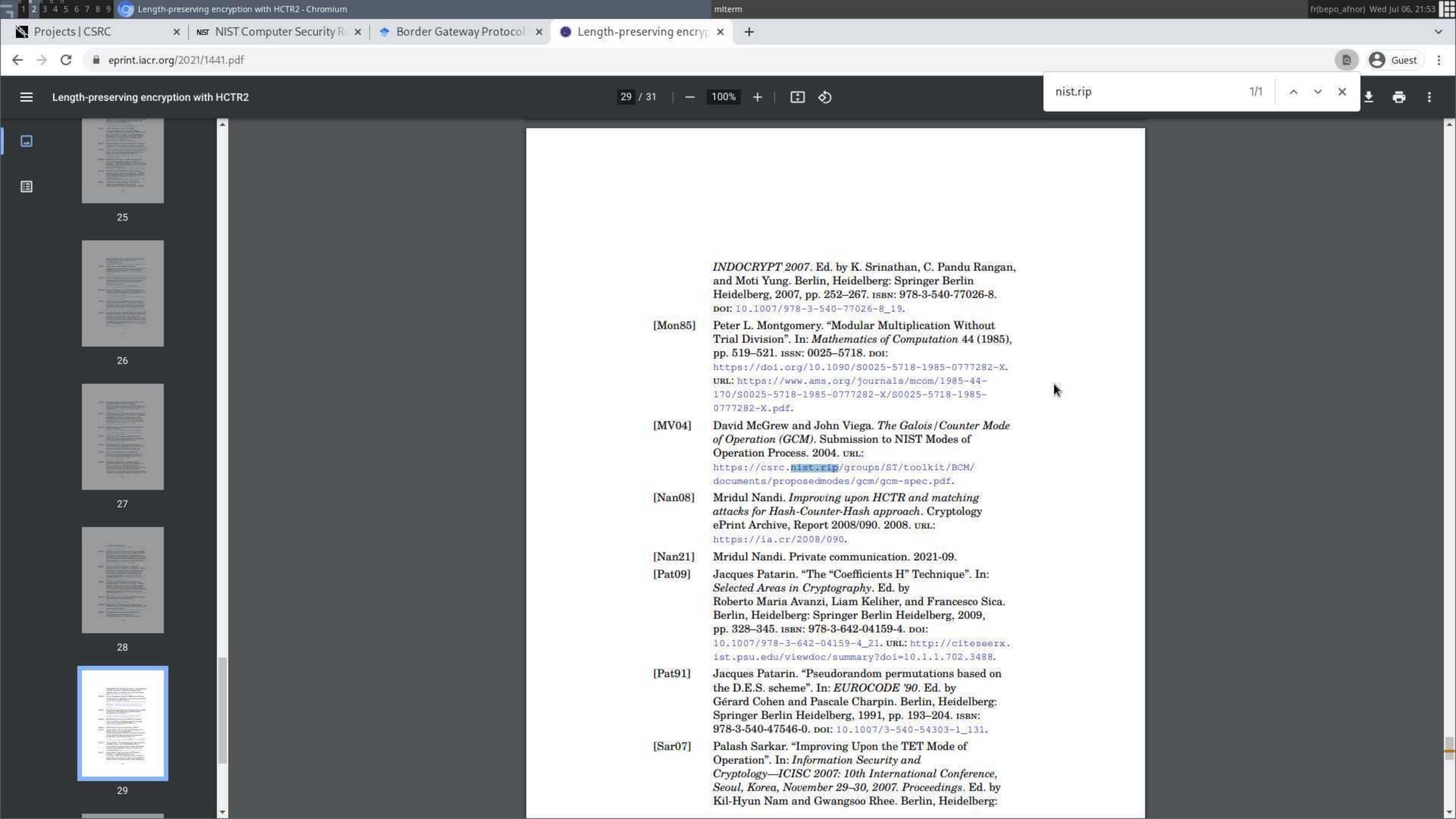
-- 4 files displayed --

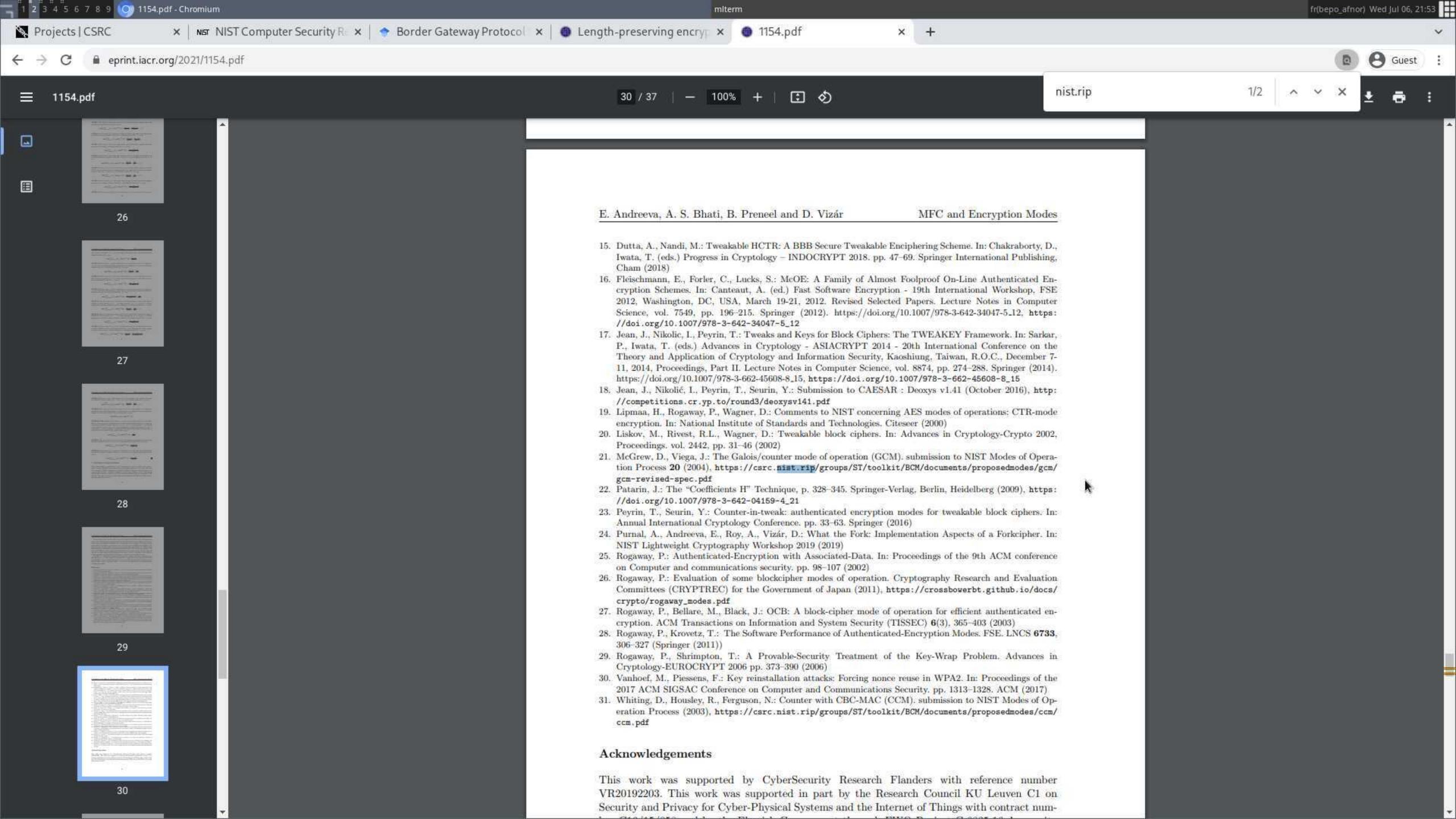
Files sourced from archive.org and fismapedia.org. Download everything here.

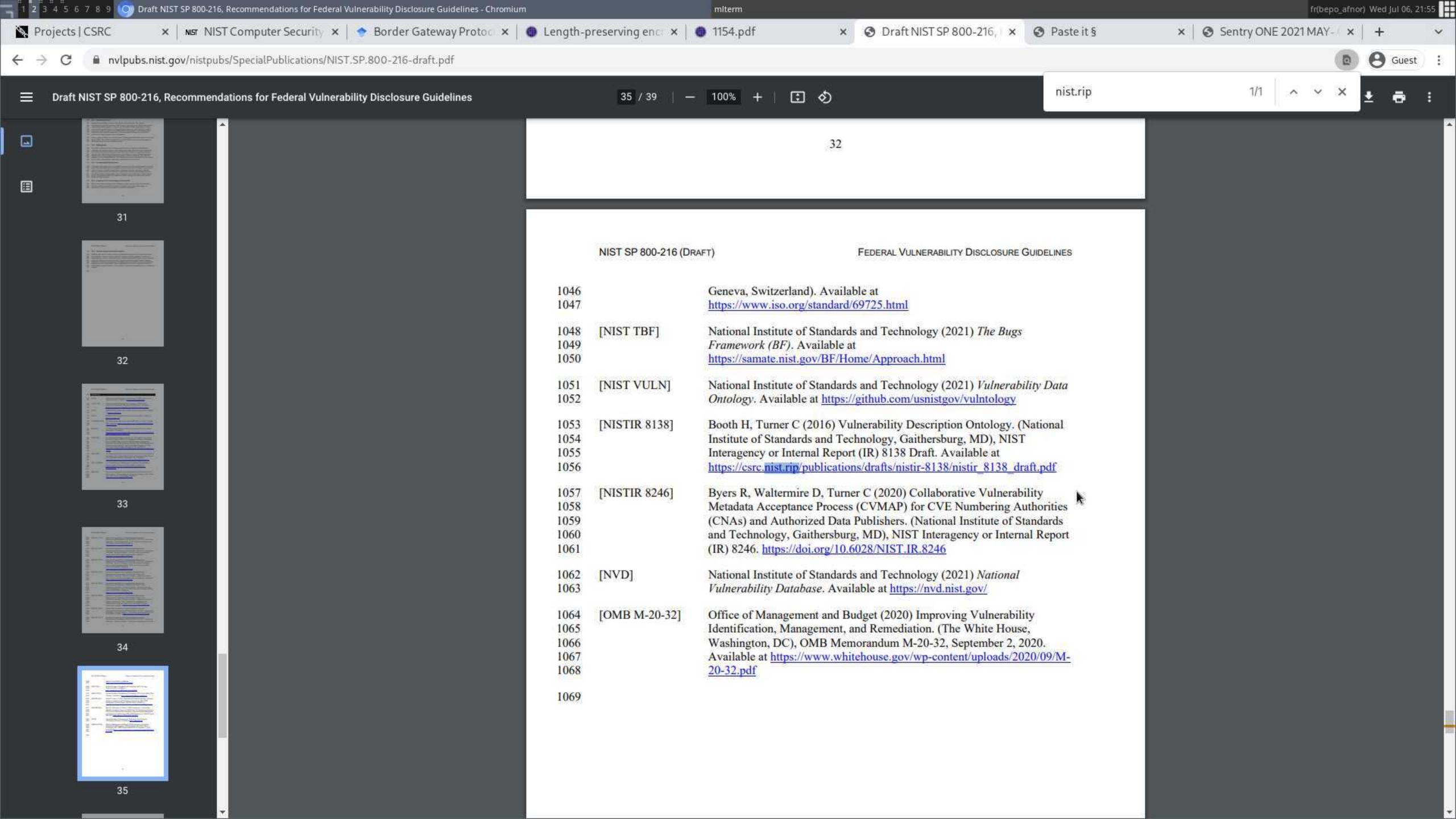
[guide] [back]

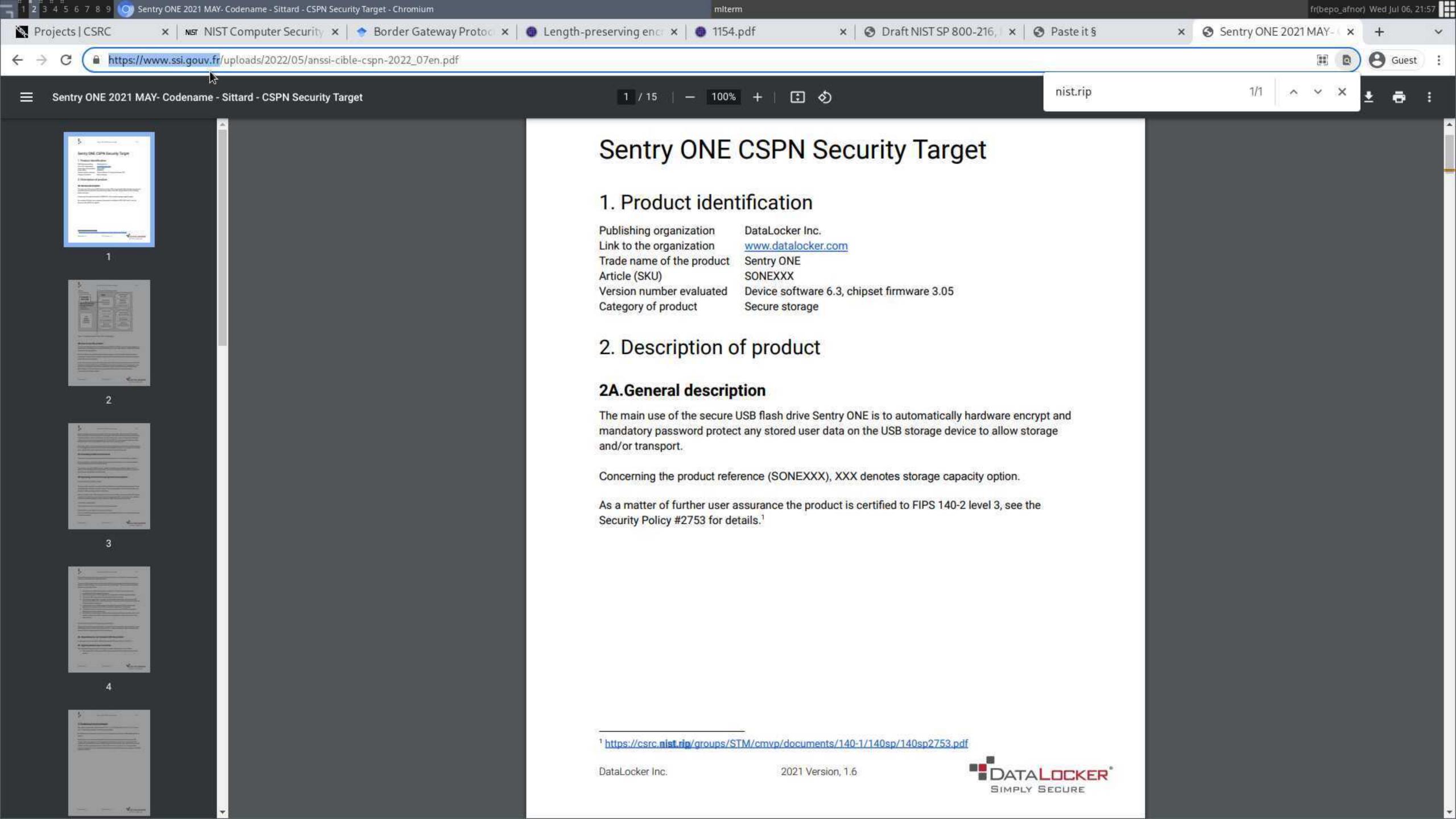


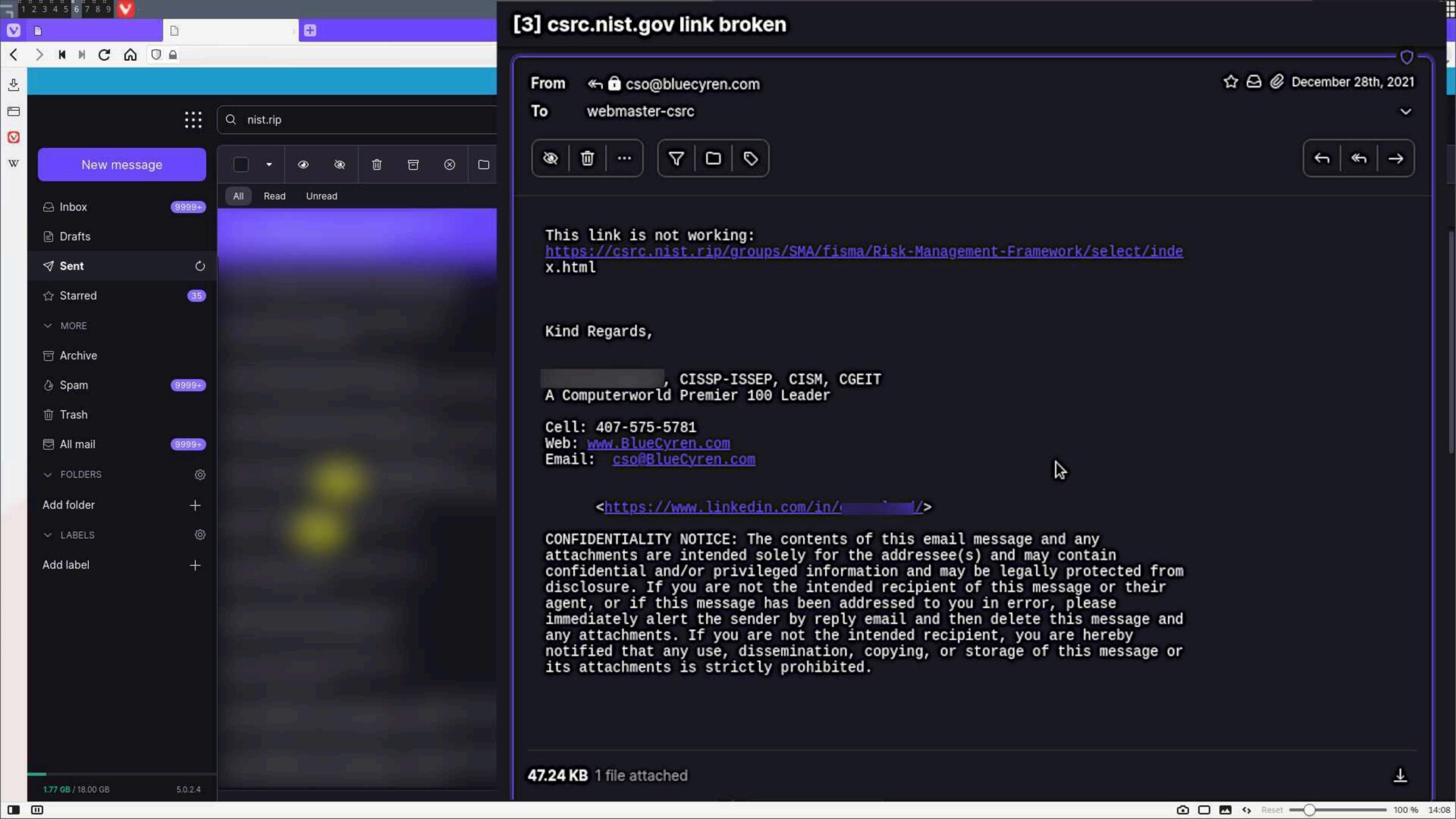


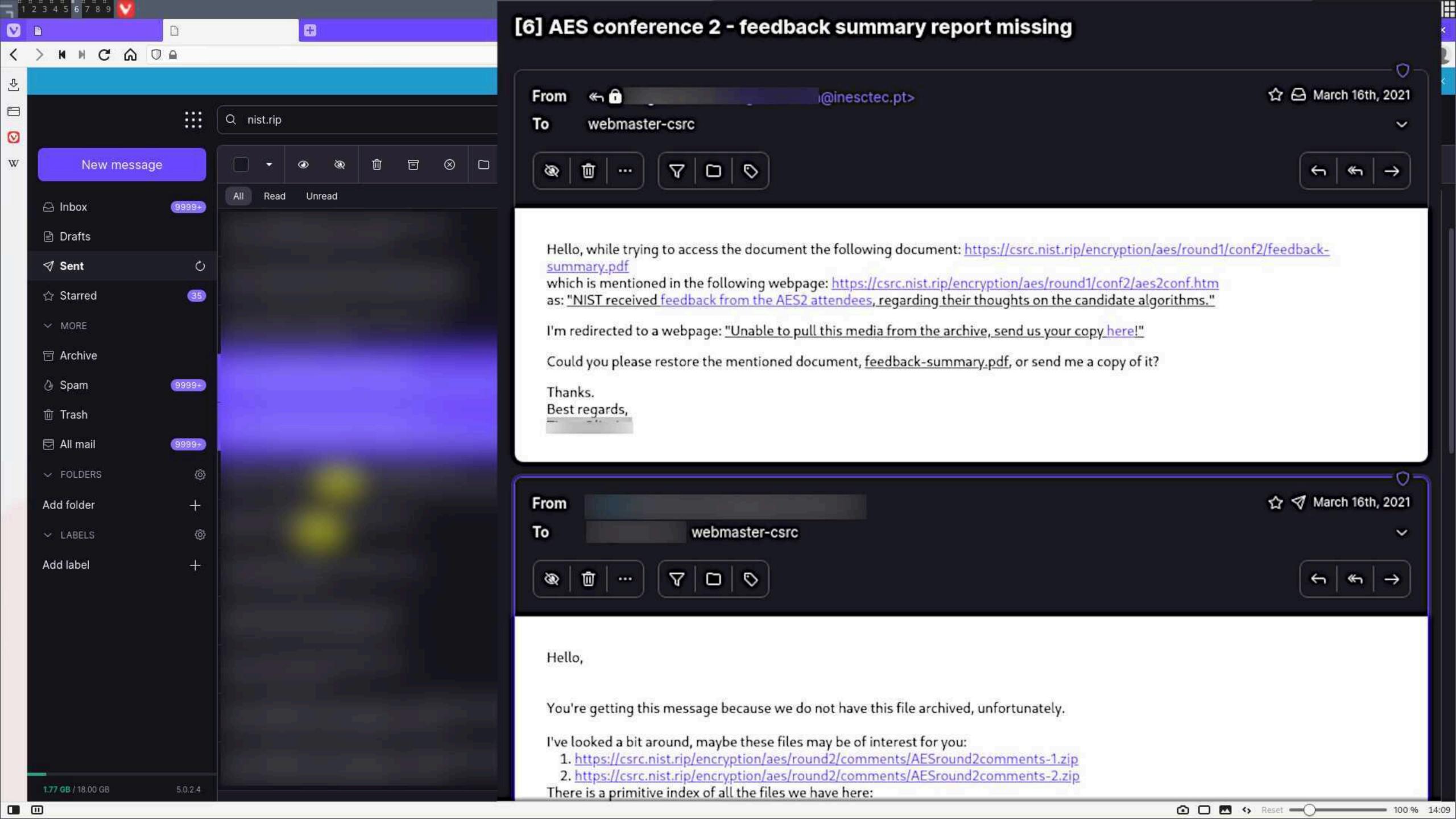


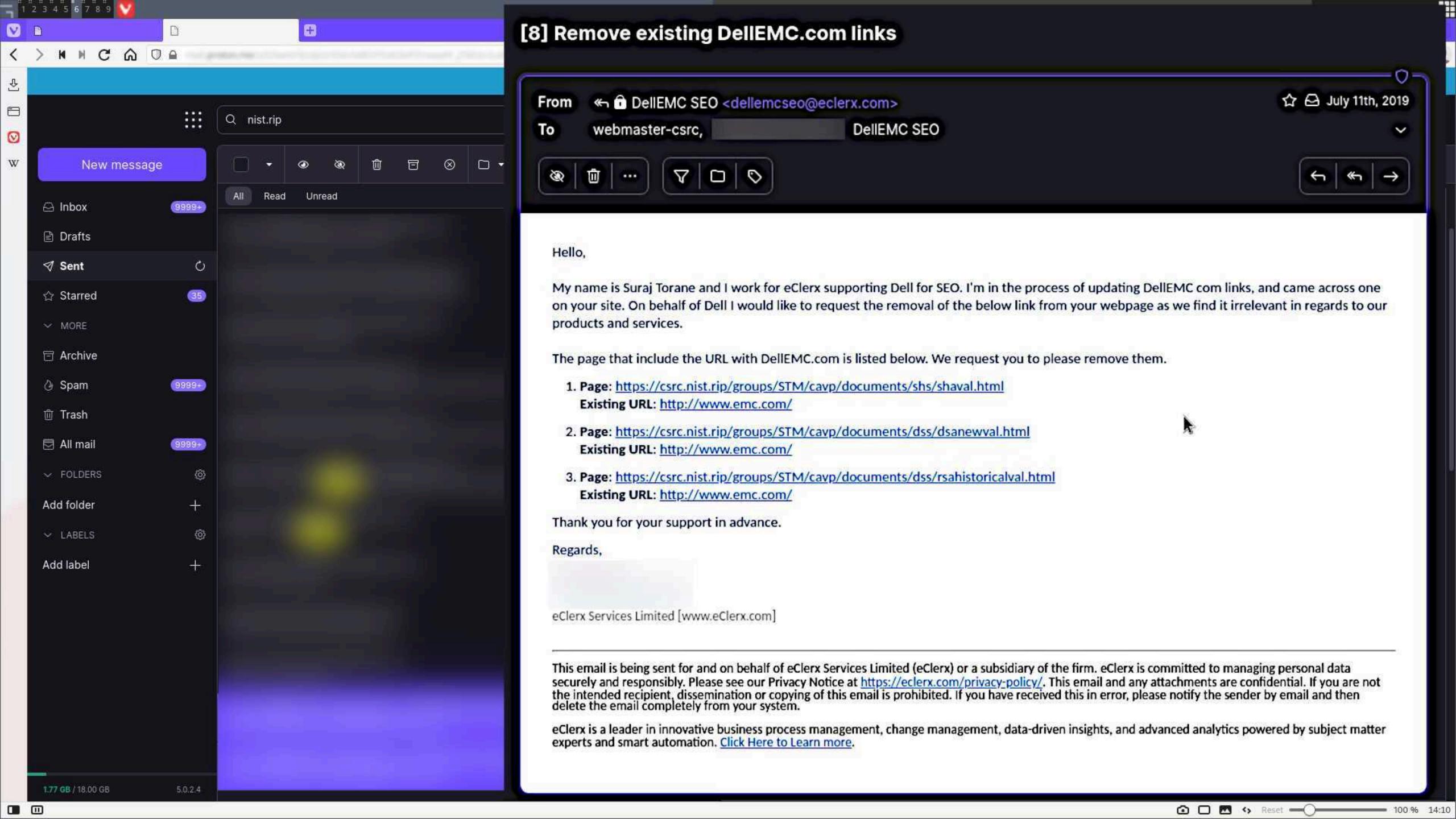


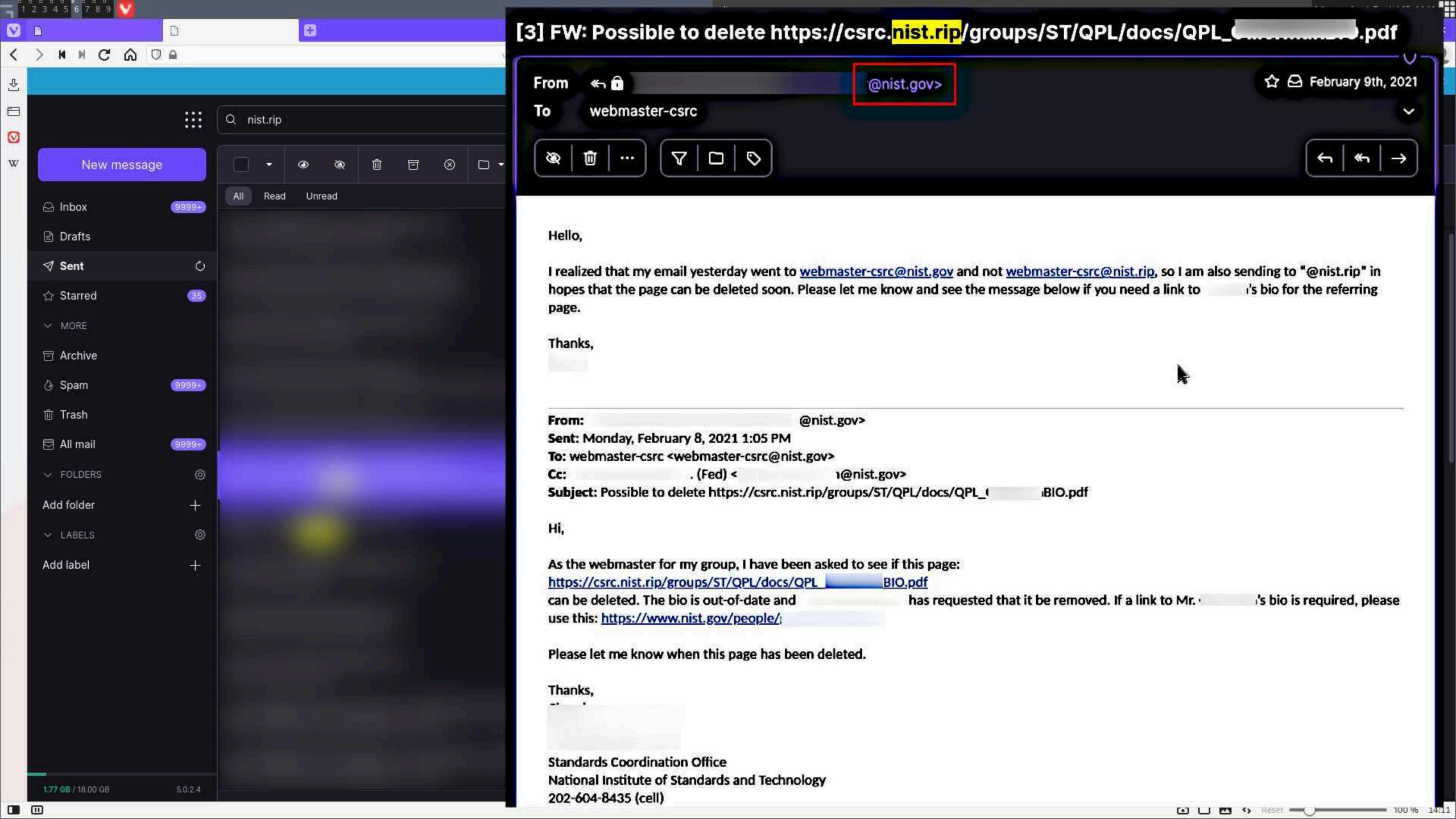












Information Technology Laboratory

# COMPUTER SECURITY RESOURCE CENTER



Projects

Publications -

Topics +

**News & Updates** 

**Events** 

Glossary

About CSRC +

#### **POPULAR LINKS**

Crypto Module Validation Program
& Validated Modules Search

NIST Cybersecurity Framework

NIST Risk Management Framework SP 800-53 Controls Site

Post-Quantum Cryptography

Publications / Drafts / SP 800s

Stakeholder Engagement / International Resources



NEW: NIST SP 800-53 CONTROLS PUBLIC COMMENT SITE



COMMENT ON DRAFT PUBLICATIONS



NIST'S "CYBERSECURITY INSIGHTS" BLOG

#### Recent updates:

- NIST updates <u>Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations</u> guidance in NIST SP 800-161r1, which also helps fulfill NIST's responsibilities under E.O. 14028. (May 5, 2022)
- Our new <u>Cybersecurity and Privacy Reference Tool (CPRT)</u> offers a consistent format for accessing the reference data of NIST
  cybersecurity and privacy standards, guidelines, and frameworks. Datasets from nine NIST frameworks and other publications are available
  and can be searched, browsed, and exported (JSON and XLSX). (May 4, 2022)
- Learn about NIST's resources for:
  - Cybersecurity Supply Chain Risk Management
  - DevSecOps
  - Measurements for Information Security
  - Operational Technology (OT) Security
  - Ransomware Protection and Response
  - Secure Software Development Framework (SSDF)
  - Vulnerability Disclosure Guidance

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related <u>projects</u>, <u>publications</u>, <u>news</u> and <u>events</u>. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

- see our greatly-expanded <u>publications library</u>,
- explore content by topic,
- search our glossary of information security terms, and
- subscribe to <u>CSRC email updates</u>.



#### Official websites use .gov

A **.gov** website belongs to an official government organization in the United States.



#### Secure .gov websites use HTTPS

A **lock** (a) or **https://** means you've safely connected to the .gov website. Share sensitive information only on official, secure websites.

25

Search CSRC Q

**≡** CSRC MENU

Information Technology Laboratory

# **COMPUTER SECURITY RESOURCE CENTER**



**Projects** 

Publications

Topics

**News & Updates** 

**Events** 

Glossary

About CSRC +



NEW: NIST SP 800-53 CONTROLS PUBLIC COMMENT SITE



COMMENT ON DRAFT PUBLICATIONS



NIST'S "CYBERSECURITY INSIGHTS" BLOG

#### **POPULAR LINKS**

& Validated Modules Search

**NIST Cybersecurity Framework** 

NIST Risk Management Framework SP 800-53 Controls Site

Post-Quantum Cryptography

Publications / Drafts / SP 800s

Stakeholder Engagement / International Resources

#### Recent updates:

- NIST updates <u>Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations</u> guidance in NIST SP 800-161r1, which also helps fulfill NIST's responsibilities under E.O. 14028. (May 5, 2022)
- Our new <u>Cybersecurity and Privacy Reference Tool (CPRT)</u> offers a consistent format for accessing the reference data of NIST cybersecurity and privacy standards, guidelines, and frameworks. Datasets from nine NIST frameworks and other publications are available and can be searched, browsed, and exported (JSON and XLSX). (May 4, 2022)
- · Learn about NIST's resources for:
  - Cybersecurity Supply Chain Risk Management
  - DevSecOps
  - Measurements for Information Security
  - Operational Technology (OT) Security
  - Ransomware Protection and Response
  - Secure Software Development Framework (SSDF)
  - · Vulnerability Disclosure Guidance

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related <u>projects</u>, <u>publications</u>, <u>news</u> and <u>events</u>. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

Information Technology Laboratory

# COMPUTER SECURITY RESOURCE CENTER



**Projects** 

Publications -

Topics +

**News & Updates** 

**Events** 

Glossary

About CSRC +

# POPULAR LINKS

Crypto Module Validation Program & Validated Modules Search

NIST Cybersecurity Framework

NIST Risk Management Framework
SP 800-53 Controls Site

Post-Quantum Cryptography

Publications / Drafts / SP 800s

Stakeholder Engagement / International Resources



NEW: NIST SP 800-53 CONTROLS PUBLIC COMMENT SITE



COMMENT ON DRAFT PUBLICATIONS



NIST'S "CYBERSECURITY INSIGHTS" BLOG

#### Recent updates:

- · Learn about NIST's resources for:
  - Cybersecurity Supply Chain Risk Management
  - DevSecOps
  - Measurements for Information Security
  - Operational Technology (OT) Security
  - Ransomware Protection and Response
  - Secure Software Development Framework (SSDF)
  - Vulnerability Disclosure Guidance

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

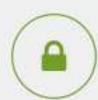
In this major update to CSRC:

- · see our greatly-expanded publications library,
- explore content by topic,
- · search our glossary of information security terms, and
- subscribe to <u>CSRC email updates</u>.



#### Official websites do not use .rip

We are an unofficial archive, replace .rip by .gov in the URL to access the official website. Access our document index <u>here</u>.



#### Secure websites use HTTPS

A lock (a) or https:// means you've safely connected to our website. Please do not share sensitive information with us.





Search CSRC Q

**≡** CSRC MENU

Information Technology Laboratory

# COMPUTER SECURITY RESOURCE CENTER



Projects

Publications

Topics +

**News & Updates** 

**Events** 

Glossary

About CSRC +



NEW: NIST SP 800-53 CONTROLS PUBLIC COMMENT SITE



COMMENT ON DRAFT PUBLICATIONS



NIST'S "CYBERSECURITY INSIGHTS" BLOG

#### POPULAR LINKS

Crypto Module Validation Program & Validated Modules Search

**NIST Cybersecurity Framework** 

NIST Risk Management Framework
SP 800-53 Controls Site

Post-Quantum Cryptography

Publications / Drafts / SP 800s

Stakeholder Engagement / International Resources

### Recent updates:

- Learn about NIST's resources for:
  - Cybersecurity Supply Chain Risk Management
  - DevSecOps
  - Measurements for Information Security
  - Operational Technology (OT) Security
  - Ransomware Protection and Response
  - Secure Software Development Framework (SSDF)
  - Vulnerability Disclosure Guidance

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

· see our greatly-expanded publications library,



#### Official websites do not use .rip

We are an unofficial archive, replace .rip by .gov in the URL to access the official website. Access our document index <u>here</u>.



#### Secure websites use HTTPS

A lock (A) or https:// means you've safely connected to our website. Please do not share sensitive information with us.



**75** 

Search CSRC Q

**≡** CSRC MENU

Information Technology Laboratory

# COMPUTER SECURITY RESOURCE CENTER



This is an archive ace .gov by .rip)

Projects

**Publications** 

Topics

News & Updates

Events

Glossary

About CSRC





5 "CYBERSECURITY INSIGHTS" BLOG

## POPULAR LINKS

Crypto Module Validation Program & Validated Modules Search

**NIST Cybersecurity Framework** 

NIST Risk Management Framework
SP 800-53 Controls Site

Post-Quantum Cryptography

Publications / Drafts / SP 800s

Stakeholder Engagement / International Resources

- measurements for information Security
- Operational Technology (OT) Security
- Ransomware Protection and Response
- Secure Software Development Framework (SSDF)
- Vulnerability Disclosure Guidance

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects**, **publications**, **news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

In this major update to CSRC:

see our greatly-expanded <u>publications library</u>,