

NIST

Computer Security Division

Donna F. Dodson

May/June 2012

Draft Publications

January 2012 – May 2012

NIST IR	NIST IR-7848	DRAFT Specification for the Asset Summary Reporting Format 1.0	May
	NIST IR-7511 Rev. 3.01.165	DRAFT Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements	April
	NIST IR-7622	DRAFT Notional Supply Chain Risk Management Practices for Federal Information Systems	March
FIPS	FIPS-186 -3 Proposed Change	DRAFT Proposed Change Notice for Digital Signature Standard (DSS)	April

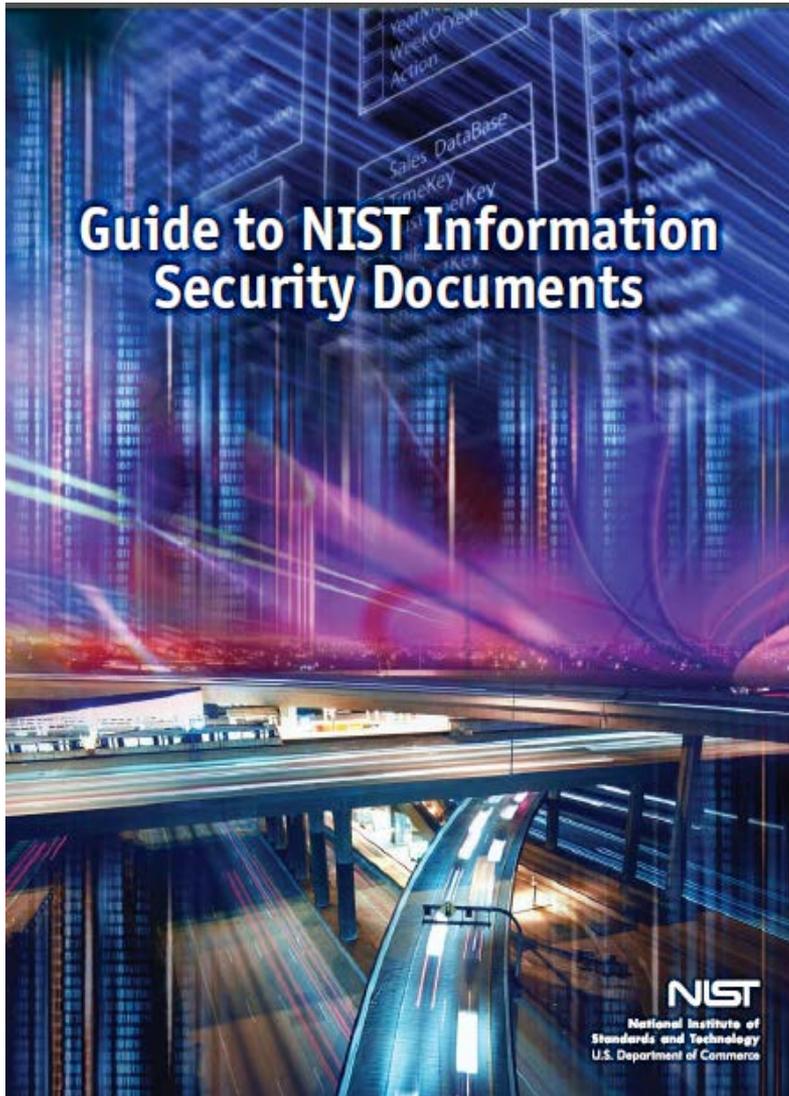
Draft Publications

January 2012 – May 2012

SP	SP 800-130	DRAFT A Framework for Designing Cryptographic Key Management Systems	April
	SP 800-66 Rev.2	An Introductory Resource Guide for Implementing the HIPAA Security Rule	In progress
	SP 800-53 Rev. 4	DRAFT Security and Privacy Controls for Federal Information Systems and Organizations (Initial Public Draft)	February
	SP 800-61 Rev. 2	DRAFT Computer Security Incident Handling Guide	January
	SP 800-18 Rev.2	Guide for Development Security Plans for Federal Information Systems and Organization	In progress
	SP 800-159	Guidelines for Access Control System Evaluation Metrics	In progress

FINAL Publications

February 2012 – May 2012



- NIST IR 7816, 2011 Computer Security Division Annual Report
- FIPS 180-4, Secure Hash Standard (SHS)

Upcoming/Recent Events

*FY12 Conferences / Workshops
Computer Security Division*

2012

- Technical Aspects of Botnets Workshop, NIST, *May 30*
- Fifth Annual Safeguarding Health Information, Ronald Reagan Building and International Trade Center, *June 6-7*
- Federal Computer Security Program Managers' Forum 2-day Offsite, June 12-13
- National Cybersecurity Center of Excellence Workshop, *June 26*
- ICT Supply Chain Risk Management (SCRM) Workshop, NIST, *July 11-12*
- Cryptographic Key Management Workshop (*Fall 2012-TBD*)

Upcoming Events

FY12 Conferences / Workshops

Computer Security Division

2012

- Revised Draft FIPS 201-2 Workshop, July 25
- Federal Computer Security Program Managers' Forum, August 9
- NICE “Shaping the Future of Cybersecurity Education” Workshop, NIST, October 30 – November 1



Past Events

*FY12 Conferences / Workshops
Computer Security Division*

2012

- NSTIC Identity Ecosystem Governance Workshop, March 15
- 25th Annual Federal Information Systems Security Educators' Association (FISSEA) Workshop, March 27-29
- Cybersecurity for Cyber Physical Systems Workshop, April 23-24

Ongoing Projects

- Small Business Information Security Outreach: For the remainder of FY12, NIST is scheduled to conduct small business information security outreach workshops in eleven states and 24 cities.

National Cybersecurity Center of Excellence (NCCoE)

Mission

To foster an environment that aligns diverse communities to adopt and utilize comprehensive cybersecurity solutions that support immediate, operational needs.

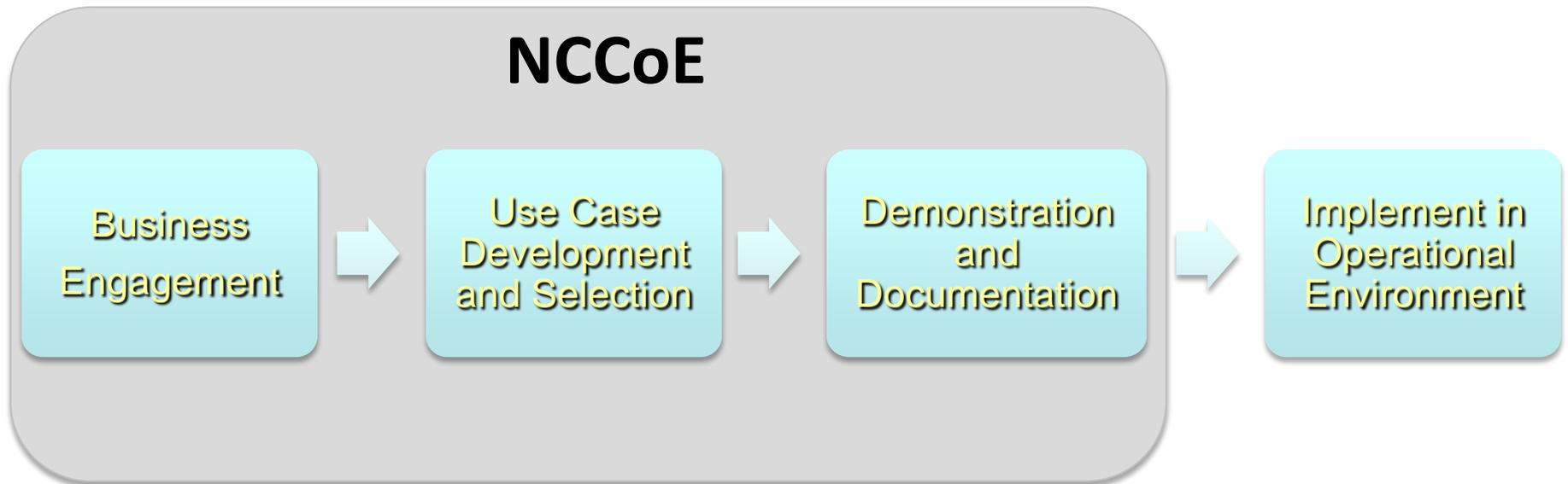




Vision

To become the benchmark for national collaborative efforts proven to deliver useful and cost effective cybersecurity solutions to the business community.

NCCoE Business Model



Governance Assumptions

Governance Board

- Critical to business engagement phase

Business Leader

- Understands current threat environment

NCCoE Exec Director

- Key facilitator working alongside Governance Board and NCCoE collaborators

High Level Goals with Objectives

Display *business* feasible
cybersecurity
principles/practices

- ...by measuring against standards to show value

Define innovation gaps

- ...by documenting and sharing use case results

Foster an environment to
exchange knowledge

- ...by hosting a modern development facility

Proposed Workshop Use Case

Business Need

- Security platform to enable exchange of electronic health information by small healthcare providers

Data and Information

- Electronic Health Information

Sectors

- U.S. Federal government and health IT community

IT Technology and Security Infrastructure Services

- Electronic Health Record (EHR) Systems
- Healthcare data exchange standards (e.g., HL7, DICOM, IHE)
- Desktop, laptop, and mobile devices (hardware root of trust)
- Operating systems and applications (secure configuration baselines)
- Security management and configuration (security automation specifications, continuous monitoring, health check)
- Data protection, identity, and key management (endpoint encryption, directory services, multi-factor authentication)
- Secure infrastructure (DNSSEC, IPv4, and IPv6)

Home

First Annual Workshop

Better Protection
Equals
Better Business

A New Model
for Partnerships

How The Center
Will Work

FAQs

Why NIST?
NCCoE Mission
More Information

Stronger Cybersecurity Through Collaboration

The National Cybersecurity Center of Excellence is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The Center brings experts together from industry, government and academia under one roof to develop practical, interoperable cybersecurity approaches that address the real world needs of complex IT systems. By accelerating dissemination and use of these integrated tools and technologies for protecting information technology (IT) assets, the Center:

- enhances trust in U.S. IT communications, data, and storage systems;
- lowers risk for companies and individuals in the use of IT systems; and
- encourages development of innovative, job-creating cybersecurity products and services.

Located near Gaithersburg, MD, the Center is hosted by the Commerce Department's National Institute of Standards and Technology in collaboration with the State of Maryland Department of Economic Development and Montgomery County, Maryland.

For more information on the Center, see our [fact sheet](#) and our [press release](#).

[News briefing video](#) for the new National Cybersecurity Center on NIST's YouTube channel.

[Maryland, NIST form cybersecurity partnership](#) video

NCCoE Website Comments
Contact [NCCoE Webmaster](#)

[Disclaimer Notice & Privacy Policy](#)
NIST is an Agency of the [U.S. Department of Commerce](#)

Page Created: February 21, 2012
Page Updated: March 1, 2012



NCCoE – Current Status

- Federal Registry Notice posted
- June 26th Workshop Event Announced
- UMD Grant for temporary space approved
- Several visits to area Cybersecurity Centers
- Core NCCoE staff identified
- Draft business model
- \$4M in support planned for FY12