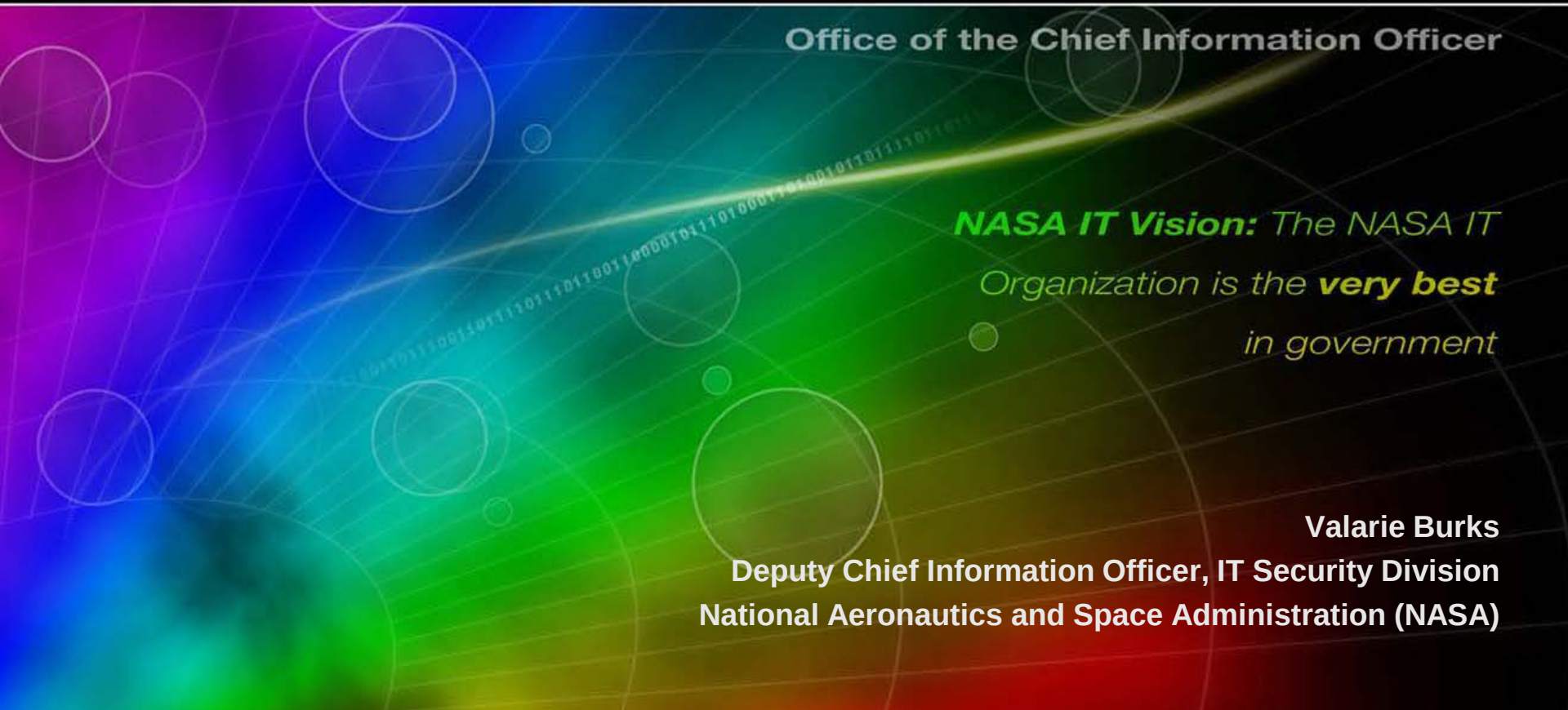
National Aeronautics and Space Administration

Enhancing NASA Cyber Security Awareness From the C-Suite to the End-User



Valarie Burks
Deputy Chief Information Officer, IT Security Division
National Aeronautics and Space Administration (NASA)

Agenda

- **From the C-Suite to the End-User**
- **The Security Education Mission**
- **NASA IT Security Awareness Campaign**
  - » Overview
  - » Goals
- **The 2013 Awareness Campaign**
  - » Leadership Projects
  - » Role-Based Projects
  - » General User Projects
- **2013 Campaign Results**
- **2013 Campaign Return On Investment**
  - » Road Show
  - » Cyber Security Expo
  - » Training
- **IREC Survey Results**
- **The Road Forward**
  - » Challenges
  - » Planned Actions

From the C-Suite to the End-User

IT security professionals alone cannot provide the needed impact on the organization's security posture – it is an ALL HANDS effort coordinated by the OCIO

- Engage Senior leadership fully:
  - » Informed of issues, challenges and compliance status
  - » Influence decisions and messaging
- Support continuing education of the security experts:
  - » Outreach to promulgate policy changes
  - » Targeted training focused on current challenges
- Engage the workforce in day-to-day security:
  - » Enhance understanding of personal role in cyber security
  - » Open communication to support cyber security collaboration

The Security Education Mission

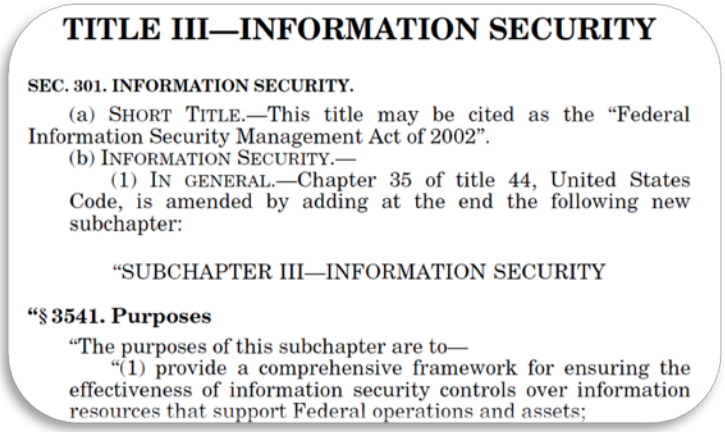
- Enhance security through improved awareness
  - » Of issues and challenges
  - » Of the impact to the organization mission
  - » Of the impact to each user's job
- Cyber Security training must make the connections among:
  - » Senior leadership business / mission imperatives
  - » OCIO policies / procedures
  - » End-User job facilitation

Cyber Security training, education and awareness programs must engage all levels and facets of the organization

Knowledge Drives Security

Regulatory Policy & Guidance

Federal Information Security Management Act (FISMA)



TITLE III—INFORMATION SECURITY

SEC. 301. INFORMATION SECURITY.

(a) SHORT TITLE.—This title may be cited as the "Federal Information Security Management Act of 2002".

(b) INFORMATION SECURITY.—

(1) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter:

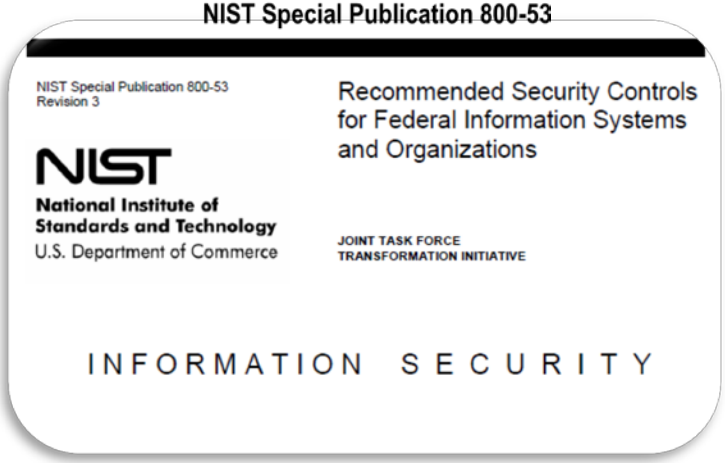
"SUBCHAPTER III—INFORMATION SECURITY

"§ 3541. Purposes

"The purposes of this subchapter are to—

"(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

NIST Special Publication 800-53



NIST Special Publication 800-53
Revision 3

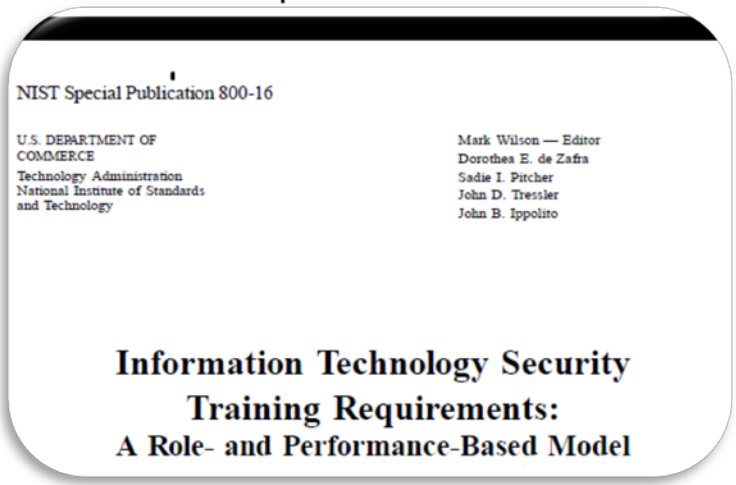
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Recommended Security Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

NIST Special Publication 800-16



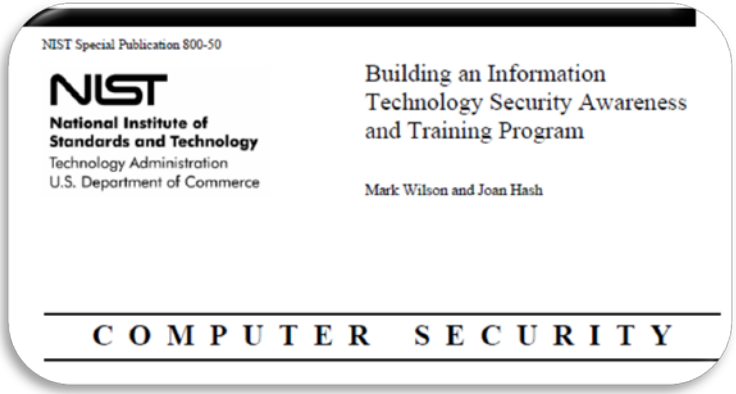
NIST Special Publication 800-16

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology

Mark Wilson — Editor
Dorothea E. de Zafra
Sadie I. Pitcher
John D. Tressler
John B. Ippolito

Information Technology Security Training Requirements:
A Role- and Performance-Based Model

NIST Special Publication 800-50



NIST Special Publication 800-50

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Building an Information Technology Security Awareness and Training Program

Mark Wilson and Joan Hash

COMPUTER SECURITY

NASA IT Security Awareness Campaign – Overview

- Improved communication and coordination on IT Security matters with Senior leadership, Center CIOs and CISOs, Mission Program directors and End-users
- Complements, not replaces the IT security training program
  - » Required periodic training typically seen as a “check in the box”
  - » Awareness campaign leverages major themes of required training and makes them “real” to employees
- Driving Security through Knowledge requires recognition that:
  - » Leadership must be engaged
  - » IT security must be personal to users
  - » Training and education efforts must be in synch with leadership messaging

NASA IT Security Awareness Campaign – Goals

- Engage and update business, mission, and IT leadership in federal compliance progress and challenges
- Improve collaboration across the Agency IT security professional community
- Communicate information security issues and challenges to the user community at-large
- Enhance targeted, role-based training for IT and IT security professionals
- Provide expanded Cyber Security awareness training to the End-User community as a whole

The 2013 Awareness Campaign – Leadership Projects

- Senior Leadership Briefings Update on annual training/awareness program
  - » Progress on compliance and strategic plan
- FISMA Awareness Briefings
  - » FISMA compliance status
  - » Leadership concerns with IT security impacts
- Cyber Security Summit
  - » Full day of workshops / panel sessions on transformation of IT / IT security
  - » Specialized training and continuing education credit per NIST SP 800-16
- Cyber Security Tips
  - » Agency CIO delivers cyber security tip to senior staff attending weekly staff meeting with Administrator

The 2013 Awareness Campaign – Role-Based Projects

- Semi-annual IT Security Advisory Board Face-to-Face
  - » Issues / challenges update and discussion
  - » Focus group meetings for ongoing projects

- IT Security Awareness WebEx
  - » Quarterly updates on federal and Agency policies, procedures, and issues for personnel with significant security responsibilities
  - » Semi-annual focused training addressing current IT security challenges

- Cyber Security Training & Certifications
  - » 3-5 day training classes on current relevant topics such as: Encryption, Privacy, Social Engineering, Cloud Computing
  - » Certification training to meet requirements for role-based training such as: CISSP, SCNP, GSEC, ITIL, CEH, MCSE, CCNA, Security+

The 2013 Awareness Campaign – General User Projects

- Annual Cyber Security Expo
  - » Events coordinated with National Cyber Security Awareness Month
  - » IT Security subject matter expert speakers available via webinars
- Cyber Security Road Shows
  - » Live, interactive training sessions on current, relevant topics
  - » Updates on Agency IT security policies and procedures
- Cyber Security Electronic Communication
  - » Tweets of Weekly Cyber Security Tips
  - » Email broadcasts of cyber security issues and training module links
  - » Distribution of a monthly IT Security Newsletter
- Cyber Security Informational Brochure
  - » Concise description of IT security programs and tools
  - » Listing of NASA directives on IT security policy / procedure
  - » Updated annually; distributed electronically and via hard copy

2013 Campaign – Results

- OCIO IT Security Division better integrated into HQ functions and activities
  - » Weekly Cyber Security Tips now anticipated by Senior Leadership
  - » Security being consulted as IT and IT-related projects are developed
  - » Active “seat at the table” with CTO and Enterprise Architecture
- More widespread interest in enterprise awareness programs
  - » IT security staff and end-user input aimed at improved completion and tracking of required training
  - » Increased coordination among Centers making previous local training more widely available across the Agency
- Improved communication among IT Security professional community has decreased time to implement new or updated enterprise policy / procedure

2013 Campaign Return On Investment – Cyber Security Expo

- Excellent participation in Cyber Security Expo across the Agency
  - » Coordinated with the DHS National Cyber Security Awareness Month
  - » Hundreds of employees attend activities sponsored at each our Centers throughout the month
    - Feedback provided is helping to improve outreach programs
    - Training was incorporated to help achieve annual training goals


Glenn Research Center


Marshall Space Flight Center


Stennis Space Center


Langley Research Center

2013 Campaign Return On Investment – Training

- Training completion statistics on the upswing
  - » 40.1% of employees completed Annual Awareness Training in the First 4 months of FY13 – compared To 31.5% in the same period of FY12

- External training sources leveraged:
  - » FISMA/NIST 3-day certification training
  - » SANS training for technical certifications
  - » Federal Cybersecurity Training Events (FedCTE) Program offerings such as Continuous Monitoring/Network Monitoring

- Applied the NICE IT Workforce Assessment for Cybersecurity
  - » Assisted in determining IT Security training requirements across the NASA IT workforce

IREC Survey Results

Areas Identified for Improvement

(Based on User responses & prioritized according to IREC Improvement Opportunity Scores)

- Present communication & training clearly and logically
- Focus training on information security policies & procedures
- Ensure that communication & training is relevant to users' day-to-day work
- Ensure that communication & training defines actions to improve security
- Ensure that training is interesting

Knowledge Drives Security

The Road Forward – Challenges

- Keep the message fresh, interesting, & relevant
  - » Ensure leadership messaging and Cybersecurity training and awareness program remain consistent
  - » Ensure communications are timely and aligned with current issues
- Assessing the impact on Users
  - » Enable the mission within a secure IT environment
  - » *Communicate, communicate, communicate!*
- Innovative methods
  - » Incorporate “wargaming” and exercises
  - » Leverage “real world” events and incidents
- Leverage NICE more fully
  - » Continue to improve partnership with DHS
  - » Ensure cybersecurity skills remain aligned with government and industry best practices

The Road Forward – Planned Actions

- Complete and analyze updated IREC survey
- Incorporate enhanced social engineering training in Road Shows
  - » Regularly scheduled penetration testing includes phishing attack scenario
  - » Leverage results of those scenarios to show: *"this is what happened to you!"*
- Leverage lessons learned from other Federal organizations gaming and exercises to enhance our training & awareness activities
- Develop FY2014 Outreach Campaign Plan
  - » Continue implementing innovative training, messaging, & delivery
  - » Leverage results of NICE/DHS workforce survey
  - » Incorporate recommendations from new IREC survey
  - » Address challenges and vulnerabilities identified by Security Operations
- Bring the message home – to the user!
- Keep the message fresh – communicate always!

Questions?

Valarie Burks
NASA Deputy CIO, Information Technology Security Division
valarie.j.burks@nasa.gov