How To Make Sense of "Significant Responsibilities" – A Draft NIST ITL Bulletin

Mark Wilson, CISSP
Computer Security Division
National Institute of Standards and Technology

- March 23, 2010 -

mark.wilson@nist.gov
(301) 975-3870 (voice)
http://csrc.nist.gov/

Making Sense

- FISMA: " . . . training and overseeing personnel with significant responsibilities for information security . . ."
- Websters Dictionary: "Significant – 1. Having or expressing a meaning : meaningful. 2. Having or expressing a covert meaning : suggestive. 3. Momentous : important."
- NIST: Train them all!

The NIST View

- NIST Information Technology Laboratory (ITL) Bulletin specifically on this topic
- April 2010 publication
- Stop-gap measure until material is incorporated into the update of NIST SP 800-50 (October 2003)
- Similar approach to training passages in the Computer Security Act

The NIST View

- User population receives annual awareness training
- Anyone with information security responsibilities beyond those that can and should be addressed in awareness training should receive formal/specialized/role-based training
- “Significant” means all those beyond the user population
- That’s anyone and everyone!

If All Are Not Trained

- As opposed to . . .
- If “significant” means some are trained and some are not . . .
  - Some personnel skills sets will not be built or developed as needed
  - Information and systems will continue to be vulnerable
  - Losses mount – data, funds, technology, lives
- Determine “significant” by first analyzing criteria?

Criteria to Consider

- Position sensitivity
- Role
- Impact level
- Greatest vulnerability
- Security controls
- Security authorization
- Security program management

Sources of Criteria

- OPM 5CFR Part 930 (June 2004)
- Position descriptions
- Performance plans
- Individual development plans
- Security plans
- Contingency plans
- Inspectors' reviews

- Thank You -

Mark Wilson, CISSP
Computer Security Division
National Institute of Standards and Technology
mark.wilson@nist.gov
(301) 975-3870 (voice)