

# Defining IT Security Requirements for Federal Systems and Networks

*Employing Common Criteria Protection Profiles in  
Key Technology Areas*

Dr. Ron Ross

# The Fundamentals

Building more secure systems depends on the use of---

- Well defined IT security requirements and security specifications  
*--- describing what types of security features we want and what the developer must do in the design and development of these features...*
- Quality security metrics and appropriate testing, evaluation, and assessment procedures  
*--- providing assurance we received what we asked for...*

# Strategic Goals

- Increase the level of assurance in Federal systems and networks in the near term by acquiring information technology (IT) products from the commercial marketplace with necessary security features and capabilities
- Promote the development of more advanced IT security products by industry in the mid-to-long term to further strengthen Federal systems and networks and create a more secure information infrastructure within the United States

# Objectives

- Develop well defined sets of IT security requirements, or *protection profiles*, in key technology areas for Federal systems and networks using the international standard Common Criteria (ISO/IEC 15408)
- Create cost-effective IT security metrics and associated methods and procedures using standardized sets of Common Criteria-based assurance requirements
- Manage inventory of protection profiles in a life cycle process to evolve with technological advancements and to protect industry investments in product development/testing
- Promote the standardization of protection profiles, wherever possible, both nationally and internationally

# Defining Requirements

## ISO/IEC Standard 15408



*A flexible, robust catalogue of standardized IT security requirements (features and assurances)*

## Protection Profiles



- ✓ Operating Systems
- ✓ Database Systems
- ✓ Firewalls
- ✓ Smart Cards
- ✓ Applications
- ✓ Biometrics
- ✓ Routers
- ✓ VPNs

*Consumer-driven security requirements in specific information technology areas*

# Principles of PP Development-I

- Security requirements will be expressed, whenever possible, using international standard ISO/IEC 15408 (Common Criteria) and be delivered in the form of protection profiles.
- Protection profiles will be targeted at high impact areas within the critical infrastructure with broad constituency support to ensure adequate participation by industry.
- Protection profiles will be developed in key technology areas, (e.g., operating systems, database systems, firewalls, smart cards, biometrics devices, public key infrastructure components, virtual private networks) and will employ a variety of security features and assurances according to projected environments of use.

# Principles of PP Development-II

- Security requirements within the same technology area, (e.g., operating systems) will be characterized, whenever possible, by a family of protection profiles, hierarchically-related to promote comparability for consumers and cost-effective testing and evaluation for industry.
- Protection profiles will be developed and vetted, whenever possible, in an open, public process in full partnership with industry, consortia, and standards groups to ensure maximum acceptance and usability.

# Principles of PP Development-III

- Protection profiles recommended for U.S. Government use will be evaluated by independent, private sector, Common Criteria Testing Laboratories and validated by the National Information Assurance Partnership (NIAP) or equivalent organizations under the international Common Criteria Recognition Arrangement.
- Protection profiles will be managed in a life cycle process with adequate transition time between versions, (i.e., new releases), to balance advances in technology against a desire for stability of requirements and to protect previous investments in product and system security evaluations.

# Principles of PP Development-IV

- Federal agencies will be encouraged to use protection profiles recommended by NIST and NSA for their respective constituencies (based upon respective authorities) according to the security and assurance needs of the organization or specific policies currently in effect.
- Protection profiles recommended by NIST and NSA will be promoted to the national and international standards communities to facilitate consensus building on security requirements for critical infrastructure protection-related applications.

# Principles of PP Development-V

- Protection profiles recommended by NIST and NSA prior to the joint development project will be grandfathered into the list of recommended protection profiles for a reasonable period of time to facilitate a seamless transition and to protect previous investments in product or system security evaluations.

# Protection Profile Matrix

Operating System PP Advanced Level	Database System PP Advanced Level	Firewall PP Advanced Level	Smart Card PP Advanced Level	Biometrics PP Advanced Level	VPN PP Advanced Level	PKI PP Advanced Level	Intrusion Detection System PP Advanced Level	Web Browser PP Advanced Level
Operating System PP Extended Level	Database System PP Extended Level	Firewall PP Extended Level	Smart Card PP Extended Level	Biometrics PP Extended Level	VPN PP Extended Level	PKI PP Extended Level	Intrusion Detection System PP Extended Level	Web Browser PP Extended Level
Operating System PP Basic Level	Database System PP Basic Level	Firewall PP Basic Level	Smart Card PP Basic Level	Biometrics PP Basic Level	VPN PP Basic Level	PKI PP Basic Level	Intrusion Detection System PP Basic Level	Web Browser PP Basic Level

**Advanced Protection**

**Extended Protection**

**Basic Protection**

## Key Technology Areas

# Protection Profile Family

Operating System PP Advanced Level	Database System PP Advanced Level	Firewall PP Advanced Level	Smart Card PP Advanced Level	Biometrics PP Advanced Level	VPN PP Advanced Level	PKI PP Advanced Level	Intrusion Detection System PP Advanced Level	Web Browser PP Advanced Level
Operating System PP Extended Level	Database System PP Extended Level	Firewall PP Extended Level	Smart Card PP Extended Level	Biometrics PP Extended Level	VPN PP Extended Level	PKI PP Extended Level	Intrusion Detection System PP Extended Level	Web Browser PP Extended Level
Operating System PP Basic Level	Database System PP Basic Level	Firewall PP Basic Level	Smart Card PP Basic Level	Biometrics PP Basic Level	VPN PP Basic Level	PKI PP Basic Level	Intrusion Detection System PP Basic Level	Web Browser PP Basic Level

**Advanced Protection**

**Extended Protection**

**Basic Protection**

## Key Technology Areas

# Potential Key Technology Areas

- Operating Systems
- Database Systems
- Firewalls
- Biometrics
- Smart Cards
- Intrusion Detection Systems
- Public Key Infrastructure
- Virtual Private Networks
- Routers and Gateways
- Web Browsers
- Telecommunications Switching Devices
- Applications

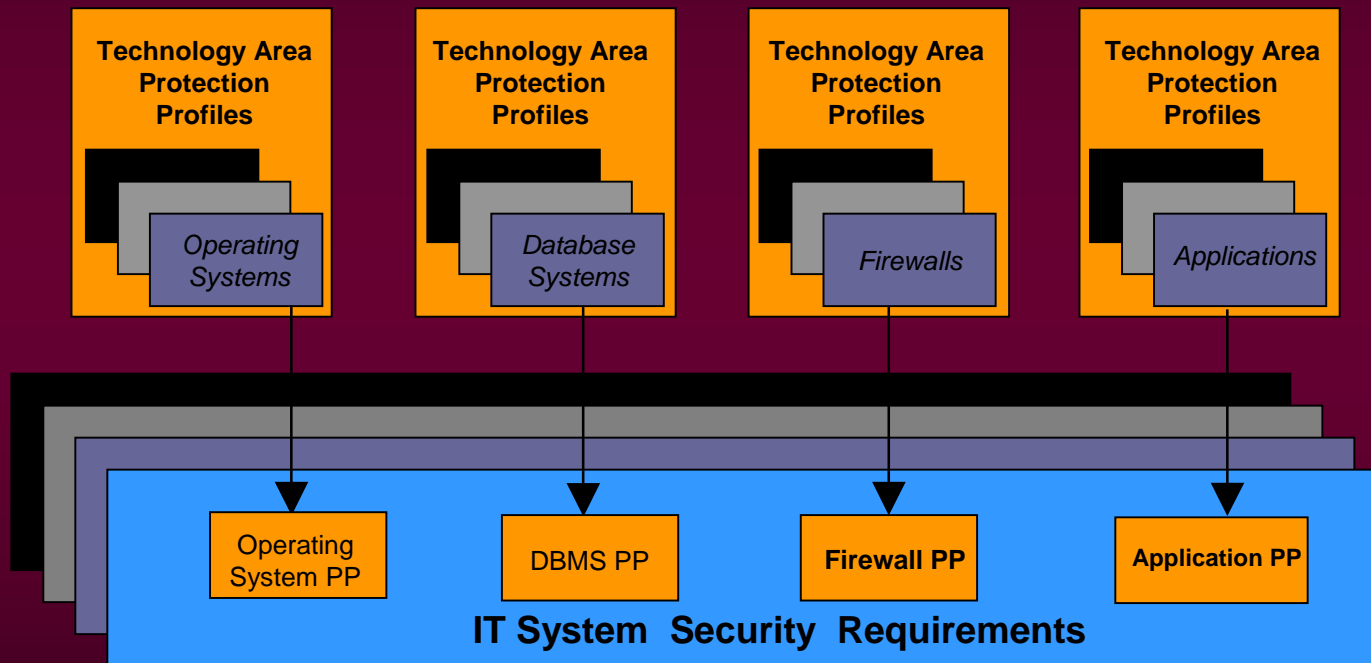
# Protection Profile Matrix

## (Characteristics)

- Protection profiles organized into *families* by key technology areas
- Protection profiles within families and across technology areas *policy* and *organization* neutral
- Three protection profiles per technology family offering *basic*, *extended* and *advanced* levels of protection
- Protection profiles *hierarchically related* within technology family

# Use of Protection Profiles

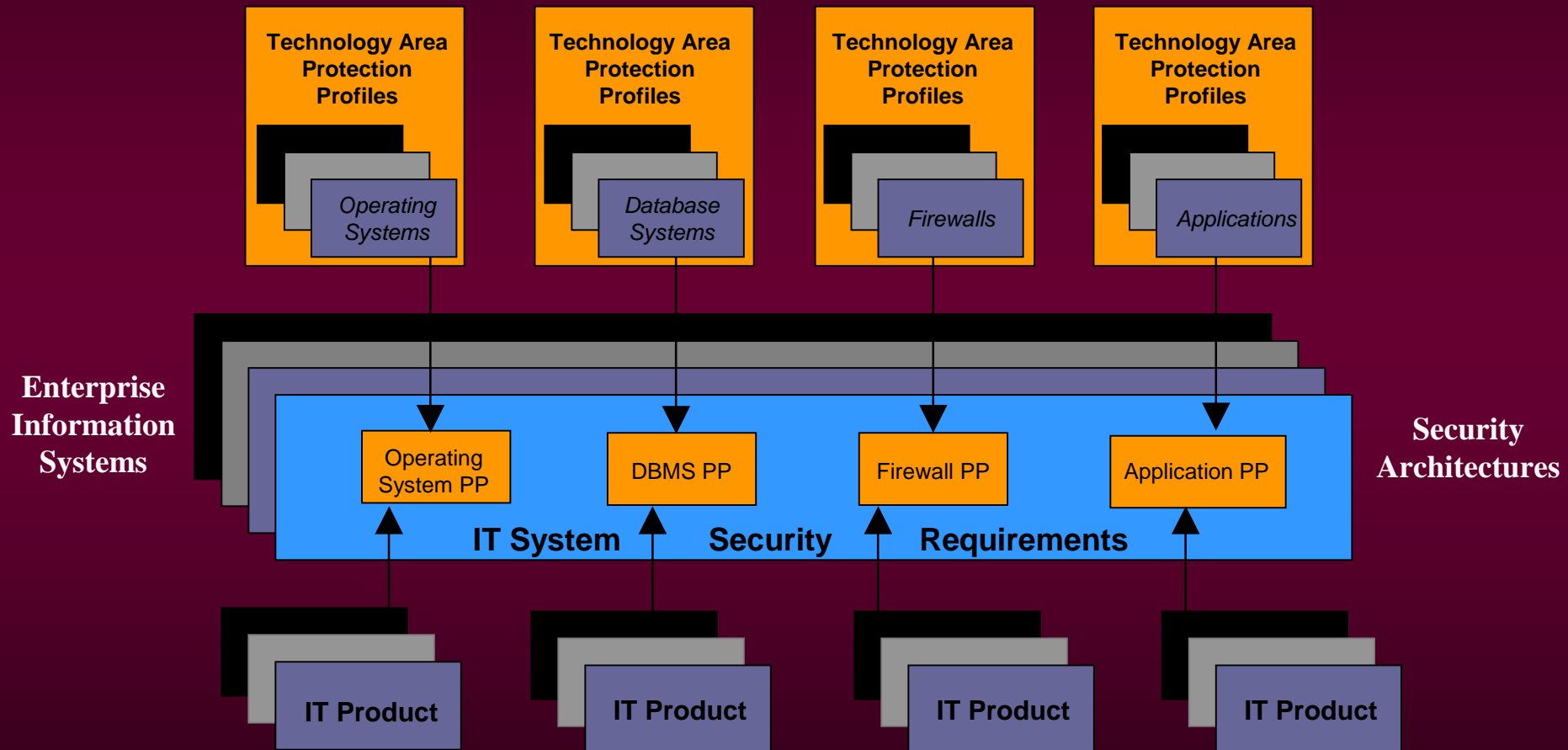
## Generalized, Consumer Driven Security Requirements



## Enterprise Information Systems

# Industry Response

## Generalized, Consumer Driven Security Requirements



Variety of Vendor Driven IT Products

NIST-NSA Technical Working Group

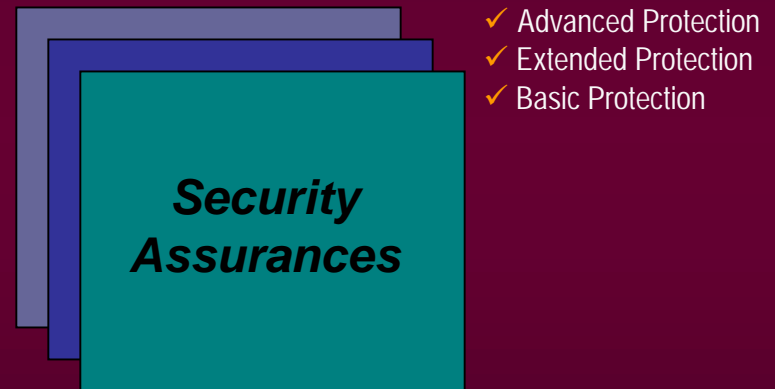
# Assurance Requirements

## Protection Profile



*Consumer statement of IT security requirements to industry in a specific information technology area*

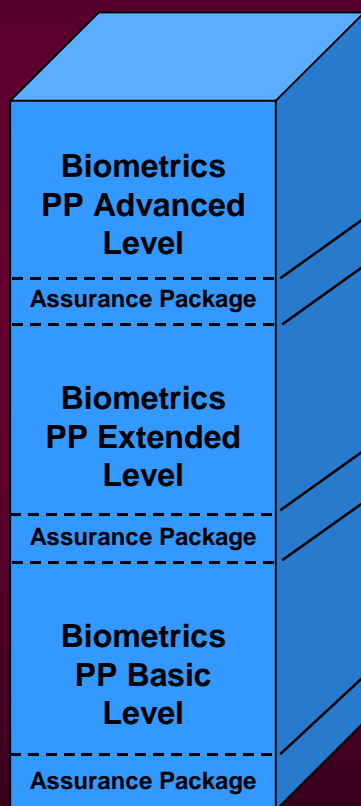
## Assurance Packages



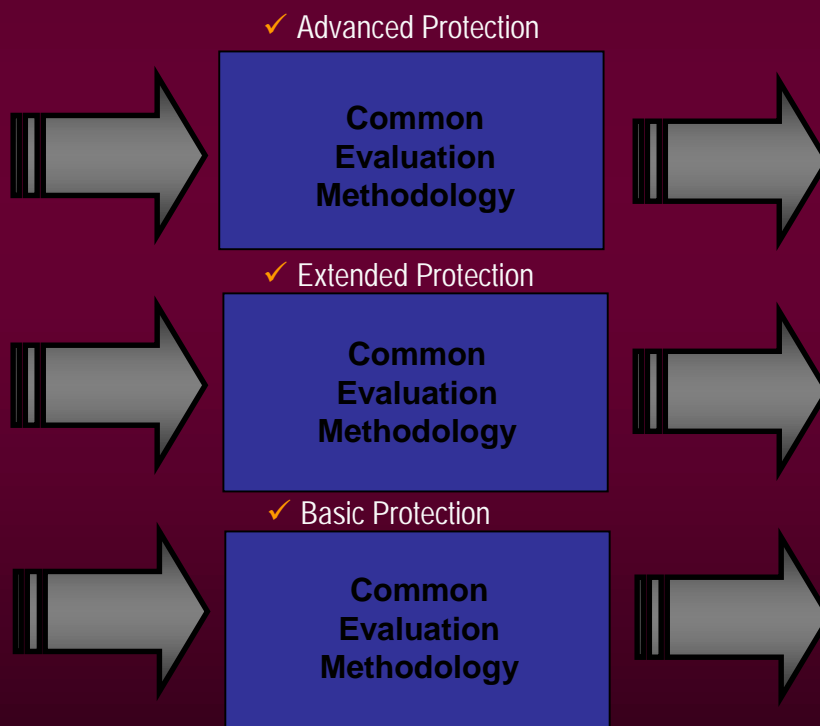
*Selection of one of three “core” assurance packages, augmented by exception when needed*

# Derived Evaluation Methodology

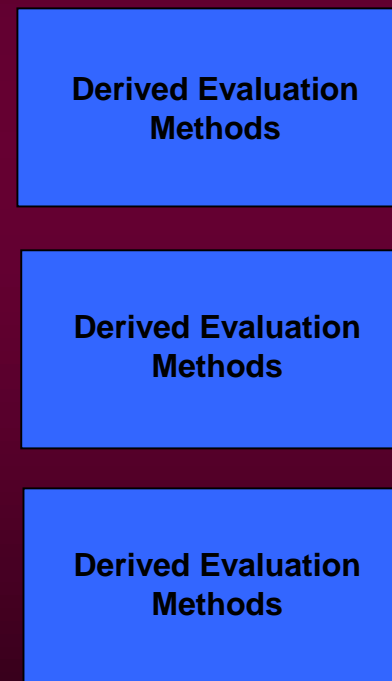
## Protection Profile Family



## Generalized Evaluation Requirements



## Technology-Specific Evaluation Methods



# Benefits of Derived Evaluation Methodology-I

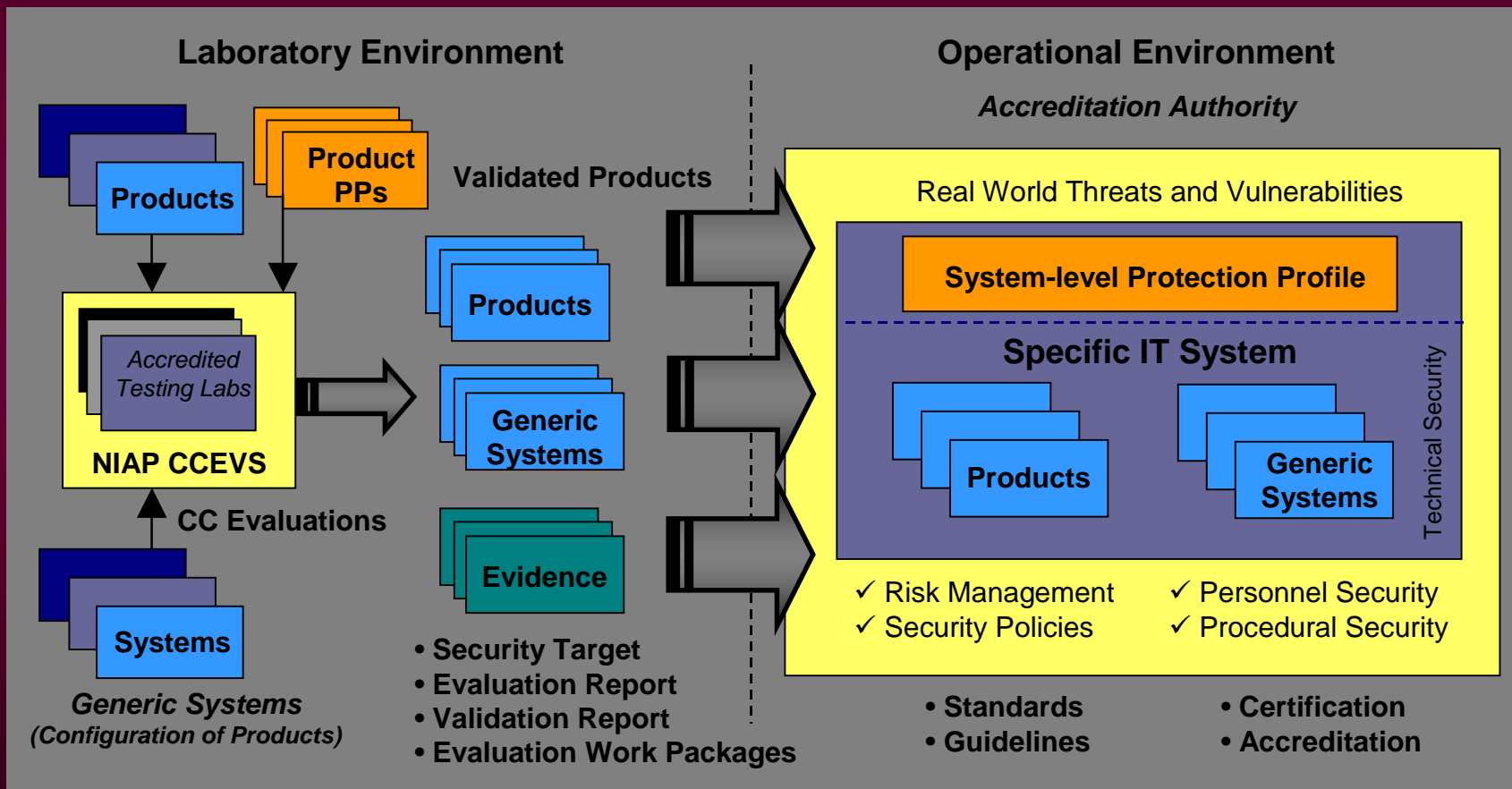
- Greater specificity in IT security testing and evaluation processes; traceable to Common Criteria requirements in protection profiles
- More objective, consistent, and repeatable IT security testing and evaluation
- More cost-effective and timely security evaluation results for consumers and producers of commercial off-the-shelf (COTS) products

# Benefits of Derived Evaluation Methodology-II

- Potential for incorporation into laboratory accreditation process to ensure competency in specialized technology testing
- Reduced need for interpretations of functional and assurance requirements and for technical oversight by validation authority
- Potential for exportability of technology-based test methods for use by Common Criteria partners and participating certification bodies leading to greater comparability of evaluations internationally

# A Comprehensive Approach

## Linking Critical Assessment Activities



# Contact Information

100 Bureau Drive Mailstop 8930  
Gaithersburg, MD USA 20899-8930

## **Director**

Dr. Ron S. Ross  
NIST-ITL  
(301) 975-5390  
[rross@nist.gov](mailto:rross@nist.gov)

## **Deputy Director**

Terry Losonsky  
NSA-V1  
(301) 975-4060  
[tmloson@missi.ncsc.mil](mailto:tmloson@missi.ncsc.mil)

## **Senior Advisor**

Dr. Stuart Katzke  
NIST-ITL  
(301) 975-4768  
[skatzke@nist.gov](mailto:skatzke@nist.gov)

## **Chief Scientist**

R. Kris Britton  
NSA-V1  
(410) 854-4384  
[rkbritt@missi.ncsc.mil](mailto:rkbritt@missi.ncsc.mil)

**Email:** [niap-info@nist.gov](mailto:niap-info@nist.gov)  
**World Wide Web:** <http://niap.nist.gov>