



**GRIFFISS  
INSTITUTE**

**NYSTEC**  
Your Independent Technology Advisor



Advice  
Strategy  
Solutions  
Consulting

*Securing the Mission of Government:  
Prevention Rather than Reaction to the Cyber Threat*

**Deborah Snyder**, NYS Deputy CISO, OITS  
**Kishor Bagul**, NYS CTO, OITS  
**Dr. Kamal Jabbour**, Senior Scientist for  
Information Assurance, AFRL  
**Slawomir Marcinkowski**, NYSTEC

**NYS Cyber Security Conference  
June 4, 2013**

NYSTEC  
500 Avery Ln, Suite A.  
Rome, NY 13441  
315.338.5818  
[www.nystec.com](http://www.nystec.com)

# AFRL Partnership

## NYSTEC's Partnership with Air Force Research Lab & Griffiss Institute

- AFRL Information Directorate - Former Griffiss AFB, Rome NY
- NYSTEC created by NYS to leverage AFRL technology & expertise
- AFRL at forefront of Cyber Security & Cyber Operations
- NYSTEC leverages this partnership to assist our NYS clients



**GRIFFISS  
INSTITUTE**





# **2013 NYS Cyber Security Conference**

**Securing the Mission of Government:  
Prevention Rather than Reaction to the Cyber Threat**

**June 4, 2013**

**Kishor Bagul  
NYS Chief Technology Officer**

# Where do we want to be?

- Efficient & Effective
- Agile for change
- Most importantly **Innovative**
  
- .....and of, course Secured!

# Where is my system?



The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.

(Gene Spafford)

[izquotes.com](http://izquotes.com)

# Do we have any challenges ?

- No **enterprise view** of the State's Information Technology portfolio
- No **enterprise architecture** and **standards** exist to guide solution design and procurement decisions
- Limited **collaboration** within and across agencies
- **Duplicate investments** made within and across agencies and no funding for upgrades.

# Nexus of forces and we are not too far from it...

- Mobility
- Information Management / Big Data
- Cloud / Shared Services
- Social Media for Government Enterprise



# **2013 NYS Cyber Security Conference**

**Securing the Mission of Government:  
Prevention Rather than Reaction to the Cyber Threat**

**June 4, 2013**

**Deborah Snyder, CISSP, CRISC, GIAC GSLC, PMP  
NYS Deputy Chief Information Security Officer**

# Change...

*“It takes a lot of **courage** to release the familiar and seemingly secure, to **embrace the new**. But there is no real security in what is no longer meaningful. There is more security in the adventurous and exciting, for in movement there is life, and **in change there is power.**”*

*- Alan Cohen (1954)*

**Got business goals?**

**Got information?**

**Got technology... cloud,  
mobile, social?**

*Got* **R R I S S K** *??*



# Driving Forces...

**Cloud**

IT Consumerization

**Collaboration**

**Mobility**

Partnerships

**Virtualization**

**Complexity**

**Innovation**

**Mandates**

**Social**

Public Expectations

**Big Data**

**Productivity**

**Data Breaches**

Economics

Culture

**Global Connectivity**

Modernization

**Intellectual Property**

**Critical Infrastructure**

# Critical Infrastructure

## Communications

- Cell Towers, Telco Switches



## Transportation

- Roads, Railroads, Bridges, Airports



## Government Facilities

- Mental Health Group Homes
- Armories



## Health and Medical Service

- Hospitals, Nursing Homes
- Adult Care Facilities



## Education

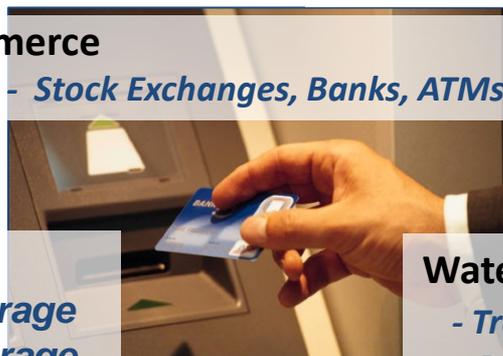
- Schools
- Colleges, Universities

## Utilities

- Gas Transmission Lines
- Electric Transmission Lines

## Commerce

- Stock Exchanges, Banks, ATMs



## Hazardous Materials

- Chemical Bulk Storage
- Major Propane Storage

## Water and Sewer

- Treatment Plants
- Dams, Reservoirs

# Critical NYS Dependencies...



# Reality Checks

- 98% of data breached (98%) came from servers
- 85% of attacks were not highly difficult
- 96% could have been avoided through simple-intermediate, low-cost controls
- 61% discovered by 3<sup>rd</sup> party, after lengthy time
- Incidents reported to the U.S. CERT increased 782% (2006 to 2012)
- >33% of organizations report employees' use of personal mobile devices lead to in malware/virus infections that infiltrated corporate networks
- Spam comprises 1 in 1.56 e-mails worldwide



**Where are we headed?**

# NYS Info-Sec Challenges

- No Enterprise Assets Inventory
- Risk Uncertainty
- Inconsistent view of business value of security
- Disparate controls & practices - Asset Inventory Management, Data Classification, Change Management, System development...
- Minimal Security Investments/Spend
- Complexity, Inefficiencies
- Inconsistent Security Services / Solutions

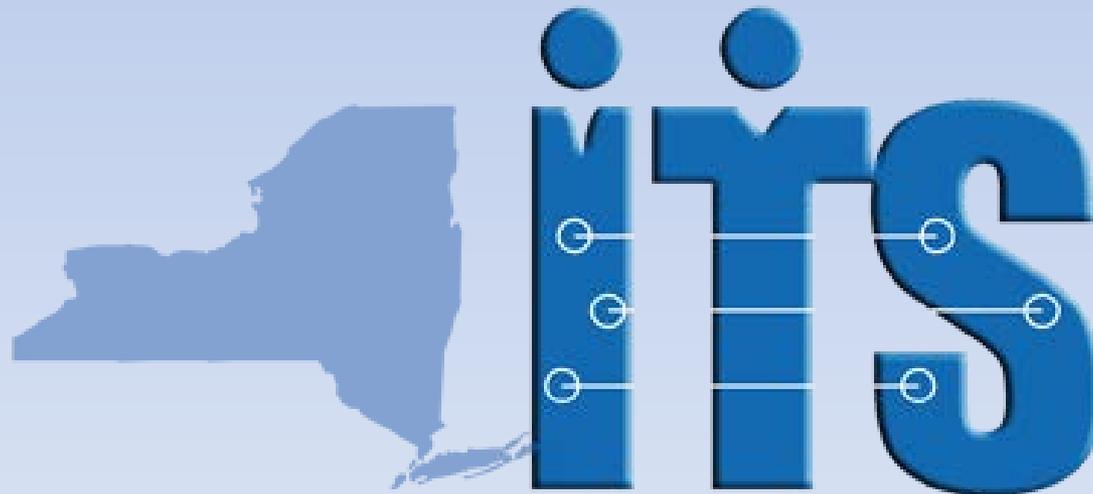
# Next-Gen Information Security

- Strategic Plan
- Pragmatic focus on key issues & critical assets
- Manage Changing Vulnerabilities & Threats
- Secure by Design
- Standardization, Automation
- Proactive Detection & Response Mindset
- Incident Readiness
- Educate & Build Vigilance

# Desired End-State

- Holistic, business-aligned, risk-based
- Mission/business functions drive decision-making, strategic considerations & investments
- Risk management & security integrated into enterprise culture, processes, architecture, engineering
- Enterprise policies, strategies
- Collaborative efforts... Innovative results

# Thank You





# Headquarters U.S. Air Force

U.S. AIR FORCE

---

## Air Force Cyber Vision 2025



**Dr. Kamal Jabbour, ST**  
**Air Force Senior Scientist**  
**for Information Assurance**

Distribution A. Approved for public release; distribution is unlimited. Public Release Case No 2012-0438

---

*Integrity - Service - Excellence*



# Cyber Vision 2025

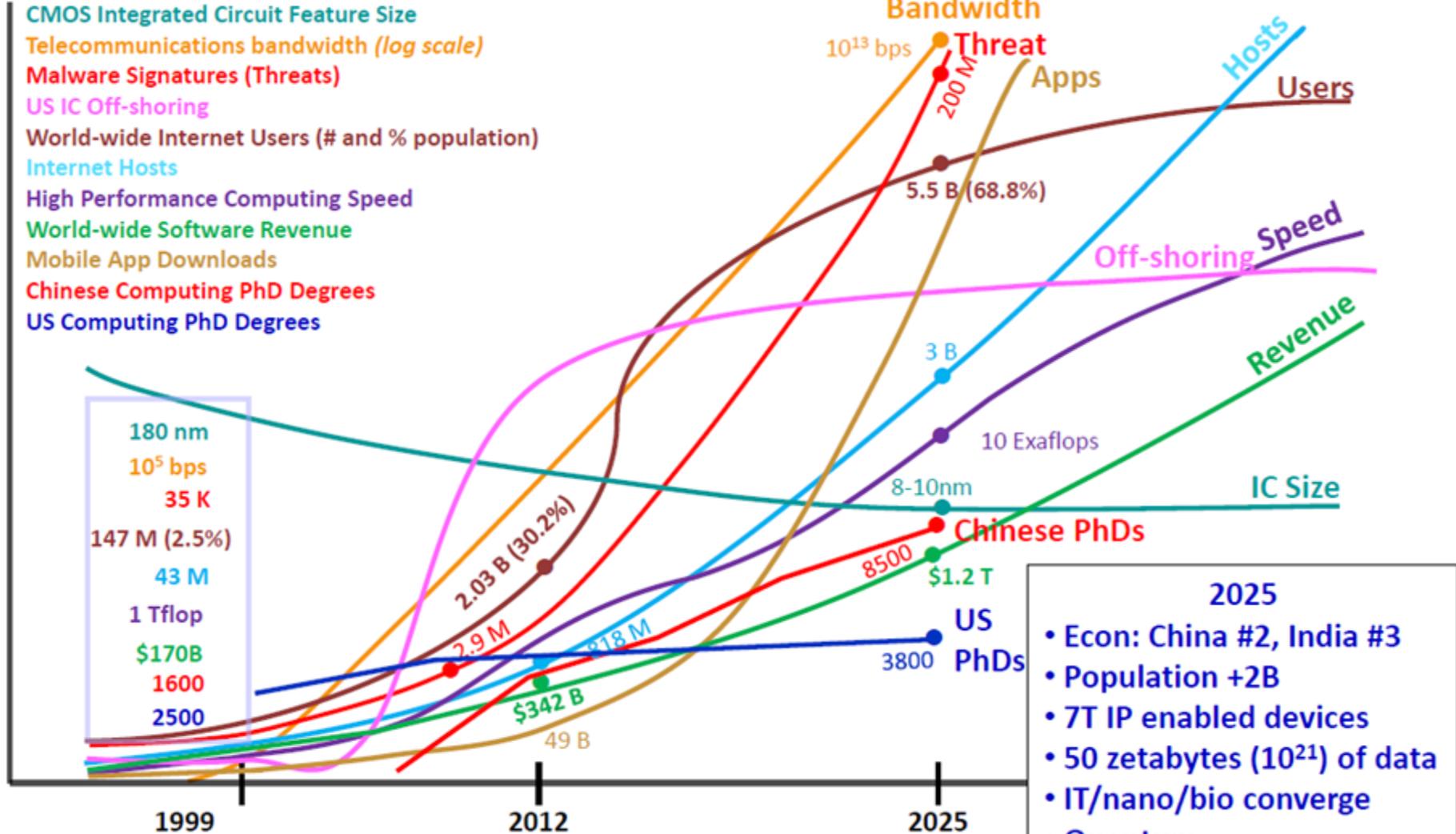
## Terms of Reference



- **Background:**
  - Need to forecast future threats, mitigate vulnerabilities, enhance the industrial base, and develop the operational capabilities and cyber workforce necessary to assure cyber advantage across all Air Force mission areas
  - An integrated, Air Force-wide, near-, medium- and far-term S&T vision to meet or exceed AF cyber goals and, where possible, create revolutionary cyber capabilities to support core Air Force missions
- **Key Stakeholders:** Air Staff, MAJCOMS, AFRL, 24<sup>th</sup> AF, ESC, ASC, SMC
- **Approach**
  - Identify state of the art and best practices in government and private sector
  - Analyze current and forecasted capabilities, threats, vulnerabilities, and consequences across core AF missions to identify critical S&T gaps
  - Articulate AF near (FY11-16), mid (FY16-20) and long (FY21-25) term S&T to fill gaps, indicating where AF should lead, follow, or watch
  - Address cyber S&T across all Air Force core missions and functions (air, space, C<sup>4</sup>ISR) comprehensively including policy as well as DOTMLPF considerations
  - Engage and partner (industry, academia, national labs, FFRDC, government)
- **Product:** Cyber S&T Vision to top 4 by 7/15/12 (Report 1/1/13)



# Future Trends 1999-2025



- 2025**
- Econ: China #2, India #3
  - Population +2B
  - 7T IP enabled devices
  - 50 zettabytes (10<sup>21</sup>) of data
  - IT/nano/bio converge
  - Quantum

CMOS – Complimentary Metal-Oxide Semiconductor; IC – Integrated Circuit  
 PhD Degrees in Computer Science/Computer Engineering/Computational Mathematics



# Environment & Findings

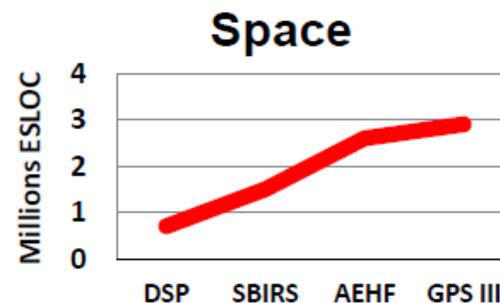
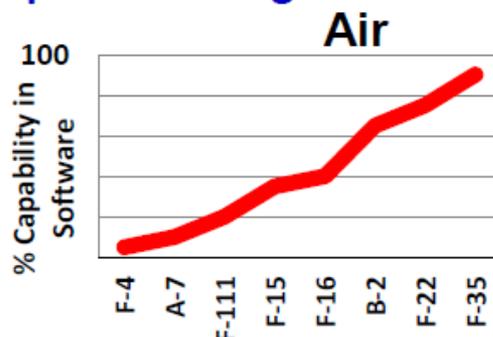


## Realities

- Our operations (air, space, C2, ISR) depend on cyber
- Cyberspace is contested and/or denied
- Resources (financial, human, time) will be constrained
- Cyber operations can have digital, kinetic, & human effects

## Findings

- **Mission at risk:** Interdependency growth driving cost and risk;  
Insider threat, supply chain threat, Advanced Persistent Threat (APT)
- Cyber S&T enables assurance, resilience, affordability, empowerment
- Need to integrate across authorities and domains
- Need to shape doctrine, policy, people, processes (RDT&E)
- Partnership and leverage essential





# Recommendations



- **Assure and Empower the Mission (MAJCOMs)**
  - Assure national security missions to security standards exceeding biz systems
  - More effective use of Title 10/50/32
  - Multi-domain synch/integrated effects
  - Increase cost of adversary OCO
- **Improve Cyber Education, Accessions, ACE (AETC, A1, A6, AFSPC)**
- **Advance Processes (AFSPC, AQ, TE, MAJCOMS)**
  - Require/design in security; secure full life cycle
  - Rapid, open, iterative acq; engage user/test early
  - Integrate cyber across CFMPs
  - Advance partnerships, align funding
- **Enhance Systems and Capabilities (AFSPC, AQ, AFMC)**
  - Reduce complexity, verify systems
  - Hardened, trusted, self-healing networks and info
  - Agile, resilient, disaggregated mission architectures
  - Real-time cyber situational awareness/prediction, managed information objects, cyber FME
- **Focused, Enabling S&T (AFRL)**
  - Assure and empower missions
  - Enhanced agility & resilience
  - Optimize human/machine systems
  - Establish foundations of trust

Area	Near (FY12-FY15)	Mid (FY16-20)	Long (FY21-25)
Conditions	<ul style="list-style-type: none"> <li>1) Measure, analyze &amp; certify</li> <li>2) Analyze, verify</li> </ul>	<ul style="list-style-type: none"> <li>1) Dynamic, resilient &amp; secure</li> <li>2) Test, train, &amp; certify</li> <li>3) Software production and deployment</li> </ul>	<ul style="list-style-type: none"> <li>1) Physical verification</li> <li>2) System verification and validation</li> <li>3) System verification and validation</li> </ul>
Agility and Resilience	<ul style="list-style-type: none"> <li>1) System risk quantification and analysis</li> <li>2) System risk analysis and mitigation</li> <li>3) System risk analysis and mitigation</li> </ul>	<ul style="list-style-type: none"> <li>1) System risk analysis and mitigation</li> <li>2) System risk analysis and mitigation</li> <li>3) System risk analysis and mitigation</li> </ul>	<ul style="list-style-type: none"> <li>1) System risk analysis and mitigation</li> <li>2) System risk analysis and mitigation</li> <li>3) System risk analysis and mitigation</li> </ul>
Human/Machine Systems	<ul style="list-style-type: none"> <li>1) System risk analysis and mitigation</li> <li>2) System risk analysis and mitigation</li> <li>3) System risk analysis and mitigation</li> </ul>	<ul style="list-style-type: none"> <li>1) System risk analysis and mitigation</li> <li>2) System risk analysis and mitigation</li> <li>3) System risk analysis and mitigation</li> </ul>	<ul style="list-style-type: none"> <li>1) System risk analysis and mitigation</li> <li>2) System risk analysis and mitigation</li> <li>3) System risk analysis and mitigation</li> </ul>
Mission Assurance and Empowerment	<ul style="list-style-type: none"> <li>1) System risk analysis and mitigation</li> <li>2) System risk analysis and mitigation</li> <li>3) System risk analysis and mitigation</li> </ul>	<ul style="list-style-type: none"> <li>1) System risk analysis and mitigation</li> <li>2) System risk analysis and mitigation</li> <li>3) System risk analysis and mitigation</li> </ul>	<ul style="list-style-type: none"> <li>1) System risk analysis and mitigation</li> <li>2) System risk analysis and mitigation</li> <li>3) System risk analysis and mitigation</li> </ul>

OCO = Offensive Cyberspace Operations; ACE = Air Force Cyber Elite; FME= Foreign Material Exploitation