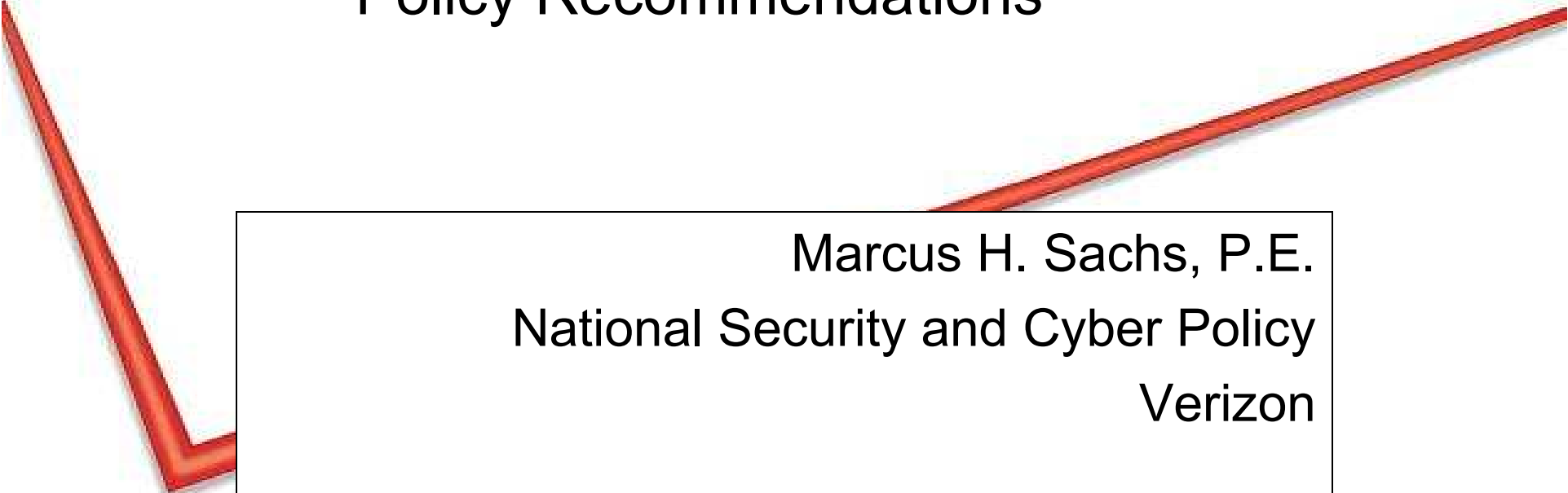




# Cyberspace Security Policy Recommendations

A large, stylized red checkmark graphic that spans across the middle of the slide, partially overlapping the text box.

Marcus H. Sachs, P.E.  
National Security and Cyber Policy  
Verizon



## Federal Cyber Security Policy Priorities

---

- Organized cyber attacks pose a significant risk to the national and economic security of the United States; however:
  - Nearly all intrusions are preventable
  - Coordinated actions by both the public and private sectors can successfully protect critical American assets
- Policy makers should focus on leveraging governmental resources to advance cyber security goals
  - While also creating incentives for the private sector to do the same



## The Federal Government Must Lead By Example

---

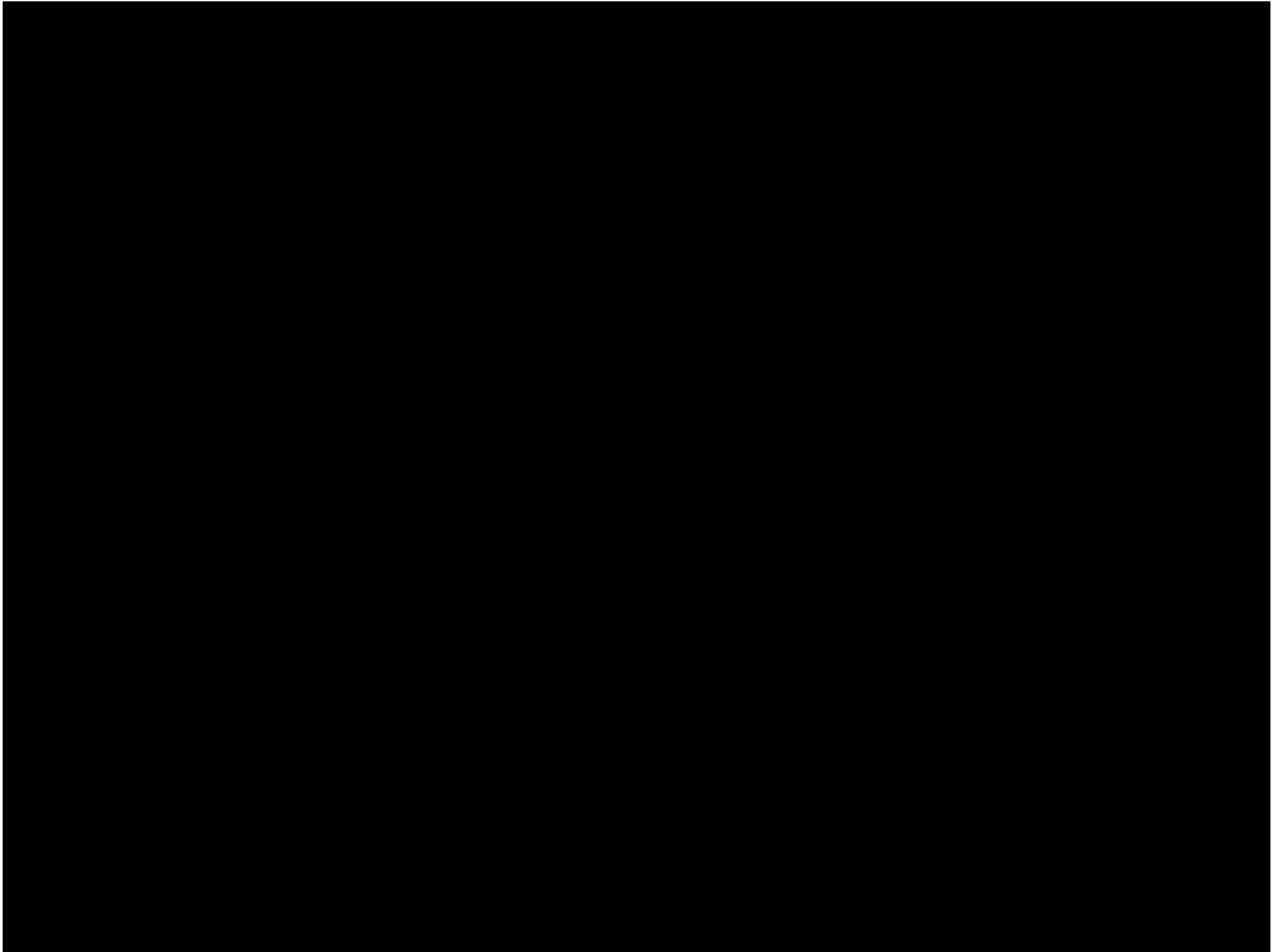
- Set the “gold standard” by managing ALL government systems in a secure manner that can be duplicated
  - .mil, .gov, and beyond
- Use acquisition powers to improve everybody’s ability to secure cyberspace
  - Be an early adopter of new security tools
  - Lowers the cost for the private sector
- Develop a career field for government cyberspace professionals, from initial entry all the way to SES
  - Security is all about the people, not the technology
- Look at cyberspace security through the lens of economics rather than just military offense/defense



## Preserve the Public-Private Partnership in Cyberspace

---

- Limit legislation and Presidential authority to the government's critical infrastructures only
  - Only include private sector infrastructure if it directly supports the government
- Any legislation or regulation must address liability, confidentiality, cost, legal conflicts, and other legitimate private sector concerns
- Terminology must be consistent (i.e., the definition of "cyberspace")
- Existing laws such as the ECPA or Patriot Act must be examined to improve the information sharing process



# Streamlining the Cyber Security Effort

Shawn Carroll  
Qwest Government Services



## Understanding the Threat

- The threat is real, credible and validated
- November 17, 2009 GAO Report GAO-10-230T  
“most agencies have not implemented sufficient controls to prevent, limit, or detect unauthorized access to computer networks, systems, or information.”
- Foreign Nations, Criminal Groups and Terrorists
- Compromise Confidentiality, Integrity and Availability of Data Systems

Government Services Inc.



## Streamlining the Effort

- Clear Policy, Strategy and Guidelines
- Redefining Critical Infrastructure
- Assess Current Methods
  - Do the current government and industry partnerships address today's needs?
- Leverage trusted advisors help solve business problems

Government Services Inc.



## What Government Can Do

- Understand where agency Subject Matter Expertise lies
- Assess current methods for securing infrastructure
- Research what services available
- Transition to services managed by SLAs and let agencies focus on mission goals

Government Services Inc.

