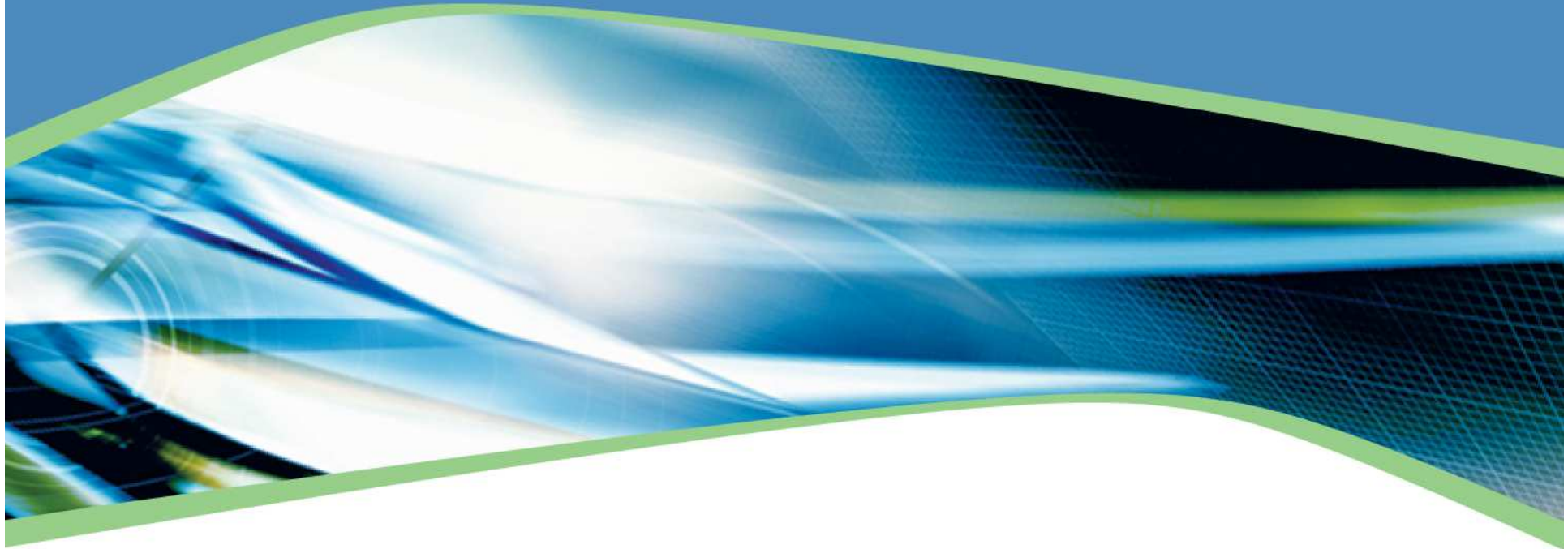


# Challenges with PIV-I

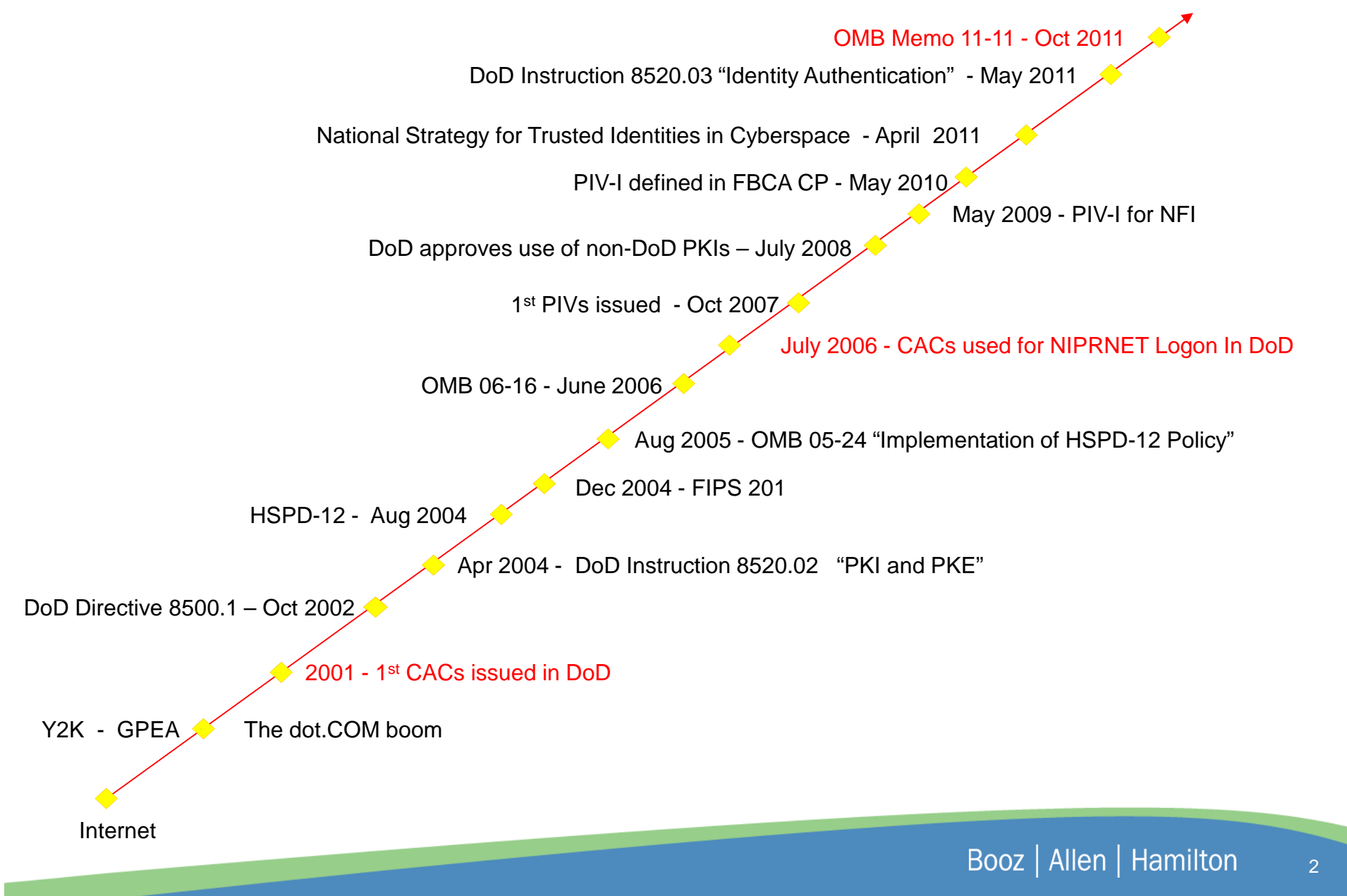
GMU C4I Center-AFCEA Symposium

23 May 2012

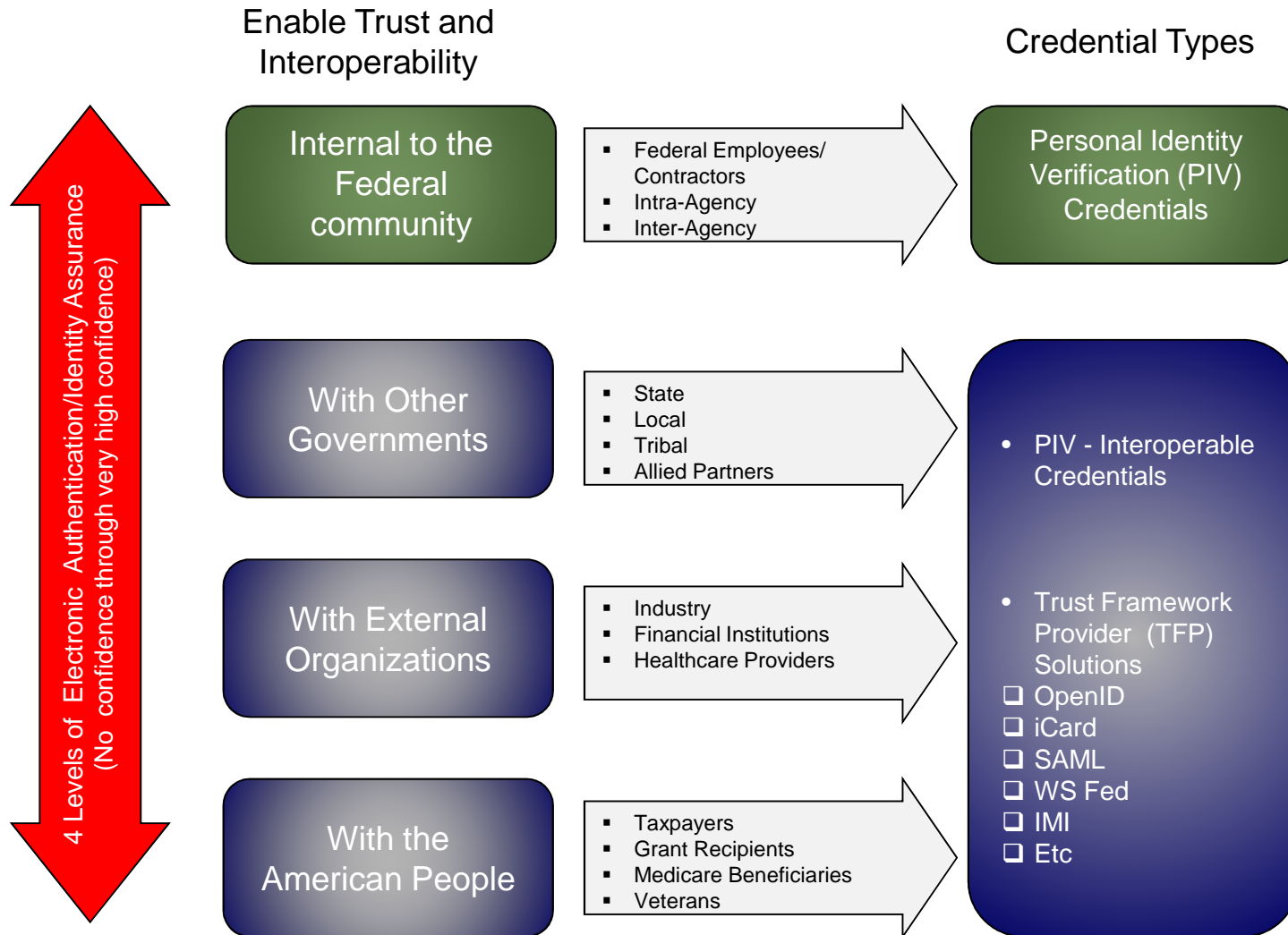
Don Fuller, Booz|Allen|Hamilton



# Implementation Lags “Policy”



# ICAM Roadmap





## WIRELESS MEDICAL DEVICES POSE SECURITY RISK

0 5

f Share Tweet

0 0

+1 Comments

Health-care providers need "robust" security programs to offset risks to wireless medical devices, says the U.S. Department of Homeland Security.

"The expanded use of wireless technology on the enterprise network of medical facilities and the wireless utilization of [medical devices or MDs] opens up both new opportunities and new vulnerabilities to patients and medical facilities," DHS warns in a **bulletin** released this month. "Since wireless MDs are now

connected to medical information technology networks, IT networks are now remotely accessible through the" medical devices.

As such, the ability of the devices' "communications security ... to protect against theft of medical information and malicious intrusion is now becoming a major concern," the bulletin continued. The increased use of such devices heightens the apprehension.

The National Cybersecurity and Communications Integration Center issued the bulletin, "Attack Surface: Healthcare and Public Health Sector."

The center cited four factors that complicate data security:

- The continued use of medical devices built before enactment of the Medical Device Law in 1976, which requires more stringent testing by the Food and Drug Administration.
- A possible lack of understanding about complex security features of newer devices, "leaving open the possibilities for exploitation through zero-day vulnerabilities or insecure deployment configurations."
- Budget constraints that prompt health-care facilities to divert money from network security.
- A failure to update device security software out of a misplaced concern about the risk to sensitive information on the devices.

Follow on Twitter  
Subscribe

### ARCHIVES

By Contributor  
By Date

By John Pulley  
May 21, 2012

0 Comments

Print this article  
Email this article  
Adjust font size

## Resolving the PIV-I challenges

- Strategies and policies are pushing to “change” how the DoD and Federal government conducts GIG-based operations
- PIV-I is a “Change Management” challenge
  - Lack of understanding and recognition
  - Lack of analysis
- Reluctance to incorporate ICAM into future planning and budgeting