OMB Update for the Information Security & Privacy Advisory Board

Michael J.Howell Jr.
Deputy Administrator, e-Gov & IT

Privacy

- Amendment to Executive Order 9397 to modify mandate to use Social Security Number as a personal identifier
- OIRA, OPM and e-Gov offices working together
- Potentially significant workload and cost
- Continues previous guidance to find, reduce, or protect use of SSN and other PII

CIO Council Privacy Committee

- Planning privacy "boot camp" modeled on CIO boot camp, for incoming Senior Agency Officials for Privacy
- Establishing "roadmap" depicting privacy related events in context with other processes and deadlines
- Compiling proven best practices into a shared web-based repository

CIO Council Security and Identity Management Committee

- Formed in FY2008
- Co-chaired by CIOs from DOJ and DON
- Purpose to coordinate and direct multitude of security and identity management policies and initiatives/projects
- Defining agenda/work plan integrating multiple previously separate activities

Trusted Internet Connections (TIC)

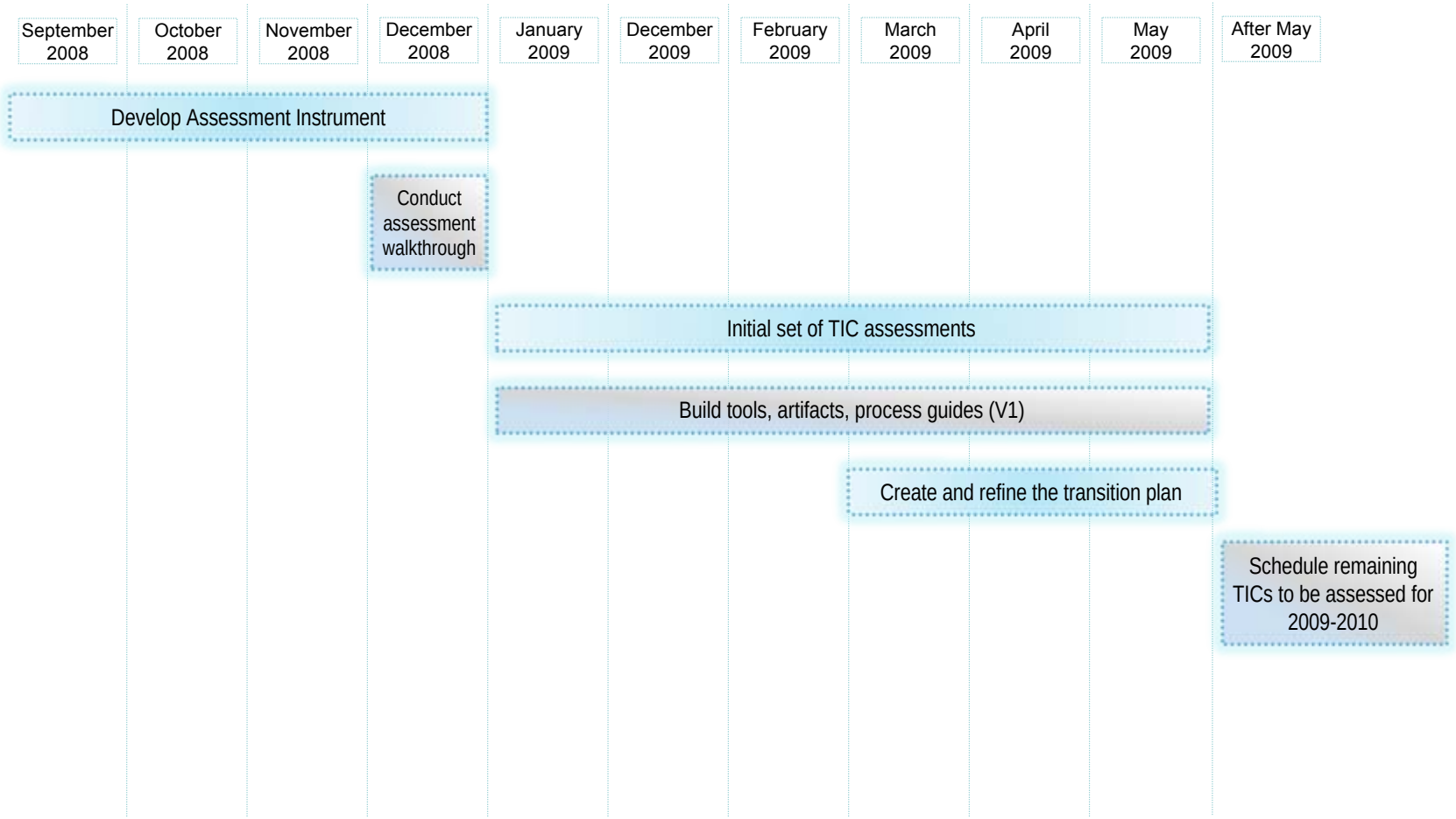
- Number of connections November 19 = reduced from 4,500+ to 2,578, target <100
- Increasingly sophisticated capabilities planned
- Networx contract modification to add TIC services – December initial award, 60 days to activate
- Includes provision of information necessary to certify and accredit
- TIC Approved Providers independently assessed to verify compliance

TIC Assessment Purpose & Output

- Purpose: provide objective, repeatable, third-party collection and evaluation of evidence from the TICAP to measure the degree of adherence to the OMB TIC requirements

- Output will include
  - Degree to which each critical OMB TIC requirement is met
  - Cumulative score = % of requirements fully met
  - Recommendation based on cumulative score:
    ≥ 90% = “Compliant”

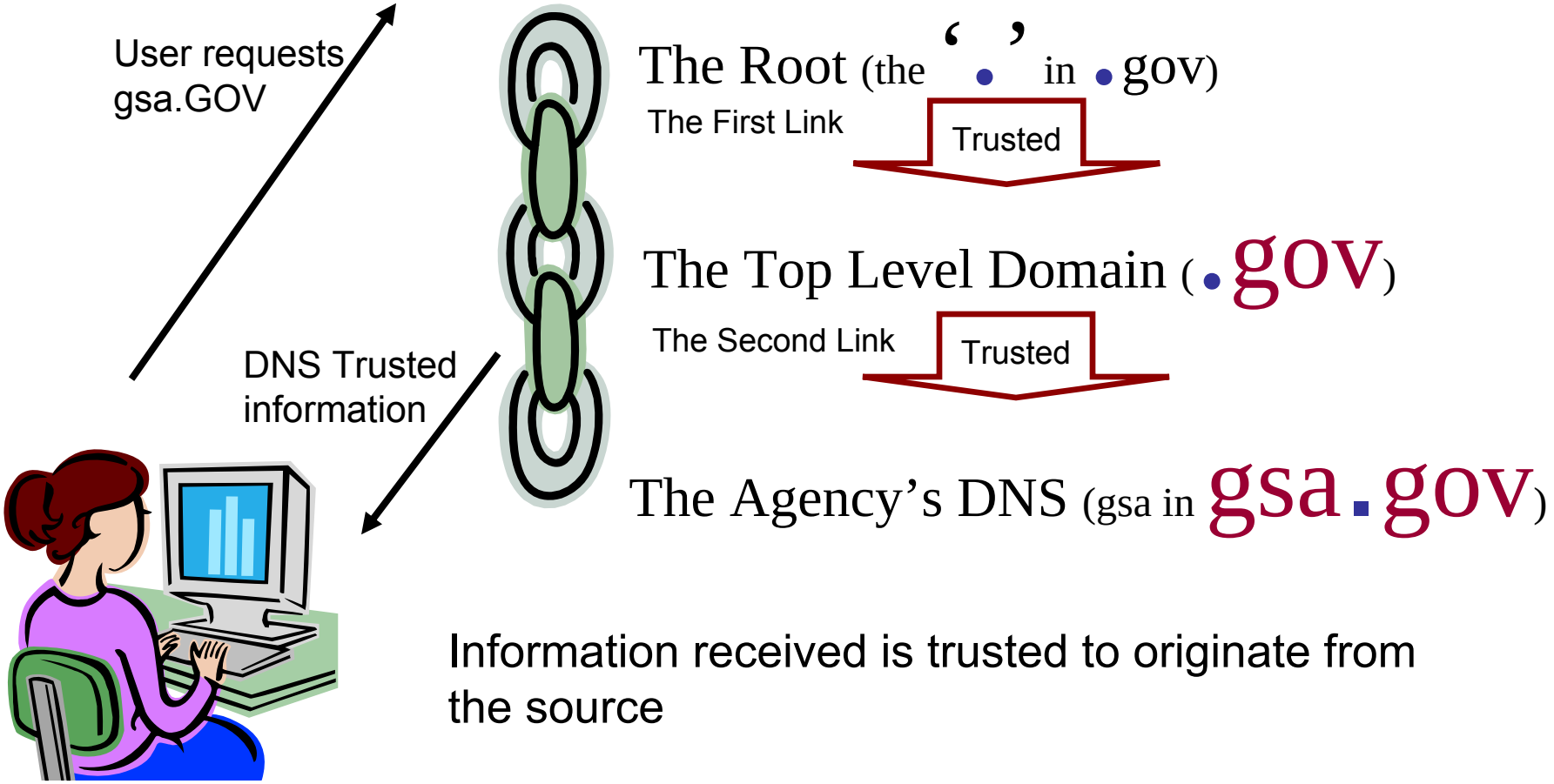
Schedule


September 2008
October 2008
November 2008
December 2008
January 2009
December 2009
February 2009
March 2009
April 2009
May 2009
After May 2009
Develop Assessment Instrument
Conduct assessment walkthrough
Initial set of TIC assessments
Build tools, artifacts, process guides (V1)
Create and refine the transition plan
Schedule remaining TICs to be assessed for 2009-2010

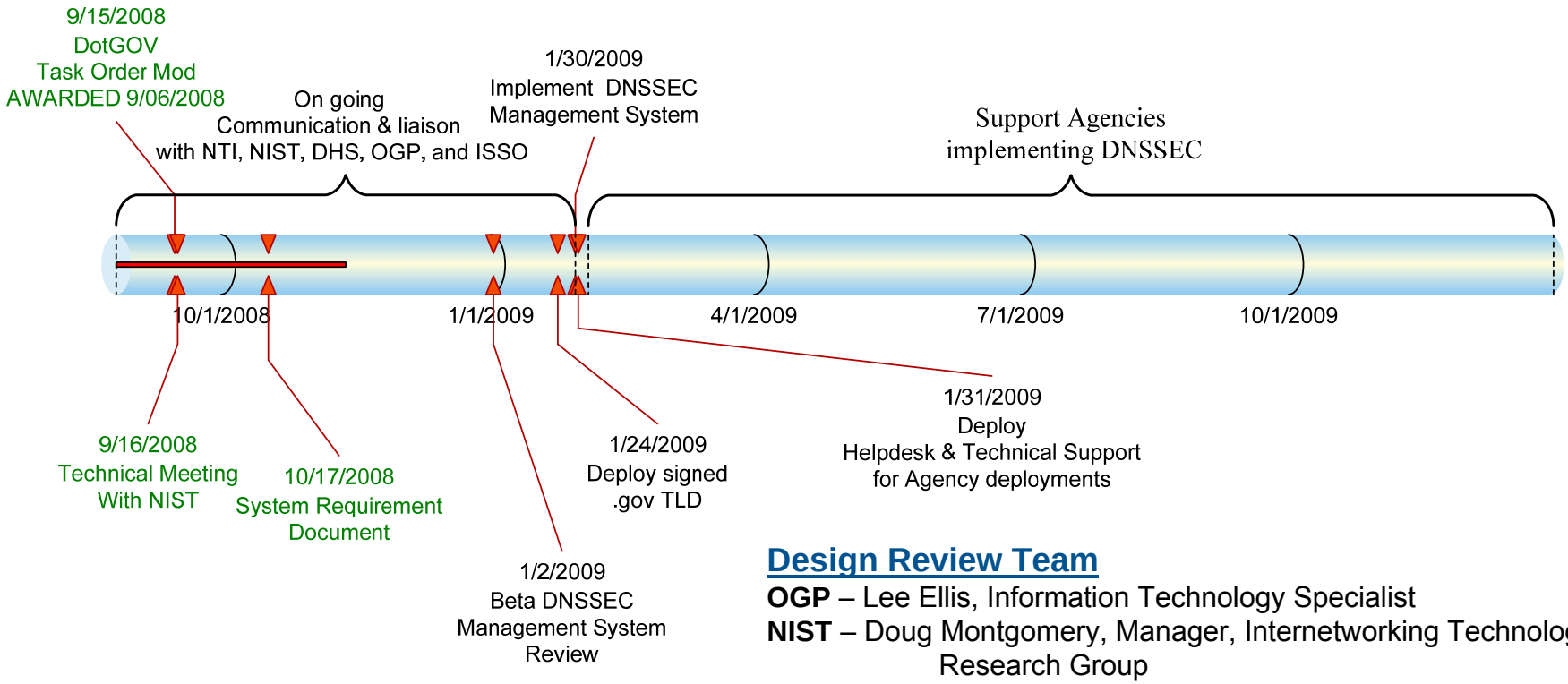
DNSSEC

- Actions in response to exposure of significant vulnerability last summer
- GSA lead for implementing DNSSEC at top level .gov domain January 2009 – on schedule
- Agencies to implement second level by December 2009
- Agency plans under review and modification

.GOV DNSSEC Deployment - Chain of Trust



.GOV DNSSEC Deployment - Schedule



Design Review Team

OGP – Lee Ellis, Information Technology Specialist
NIST – Doug Montgomery, Manager, Internetworking Technologies Research Group
Scott Rose, Computer Scientist
GSA – Daisy Bhagowalia, .GOV Program Manager
Doug Hansen, IT Management Specialist
Anthony Konkwo, FAS CISO
DHS– Chad Hinkle , IT Management Specialist
NTI – Gregg Giordano, CTO

Federal Desktop Core Configuration

- Mandatory standard security settings for Windows XP and Vista operating systems
- Monitoring implementation via Secure Content Automation Protocol
- Policy Utilization Assessment (PUA) piloted by GSA to measure actual implementation
- Next phase – extend pilot to additional agencies in December
- Potential future expansion to other platforms

HSPD-12

- October 27 2008 target date for credentialing employees
- Over 1.5 million employees and contractors credentialed (about 28%)
- Half of agencies met targets
- Internal & vendor production issues
- Remedial action plans due Nov. 17
- Future performance tracked against updated plans

Information System Security Line of Business

- Focused on automating training, managing FISMA compliance, situational awareness and incident response, and security solutions for system lifecycle.
- Good progress in 2008
- Instrumental in TIC activities
- Evaluating Smart Buys for common tools
- May be impacted if FISMA is modified – pending legislation – e.g. continuous monitoring

IT Infrastructure Line of Business

- Focused on end user computing and support, mainframes and servers, and telecommunications in 2008
- Collected initial cost and performance benchmark information
- Agencies developed initial optimization plans
- Infrastructure changes may impact security and vice versa e.g. Networx and TIC for telecomm

Upcoming Issues

- Transition
  - Chief Technology Officer?
  - National Cyber Security Advisor?
  - Changes in Priorities and Direction?
- Pending legislation
  - e-Gov Act reauthorization
  - FISMA II
  - Strengthening Transparency and Accountability in Federal Spending Act of 2008
- Collaboration, Transparency, & Government 2.0
  - e.g. National Health Dialogue
- Technology changes – Virtualization, Cloud Computing, Mobile Computing, Software As a Service, etc.