U.S. General Services Administration

Federal Acquisition Service

Integrated Technology Services

Information Security

Karl Krumbholz
Acting Deputy Director Network Services Programs
Anthony Konkwo
Information Systems Security Manager

January 30, 2007

Agenda

- Karl Krumbholz
  - Background
  - Issues and Status
  - GSA Security Approach
- Anthony Konkwo
  - GSA Compliance Monitoring
  - OSS Boundaries
  - OSS Certification

Background

- Information Security is a Global Concern
  - The Federal Information Security Management (FISMA) Act of 2002 addressed network security and mandated yearly audits
- Agencies raised concerns regarding FISMA requirements
  - Possible costs and transition delays
- Specific concerns
  - Responsibility for C&A and associated costs
  - Need to C&A of provider’s backbone (the public network)
  - C&A of provider’s operational support systems (OSS)
  - Responsibilities of Contracting Agency (GSA for Networx)
- IMC members formed a Security Working Group (SWG) to address issues and recommend solutions
  - SWG identified major 4 issues
  - Requested OMB dissemination or concurrence

Issues and Status

- Issue 1: Impact of transition on existing C&As
  - SWG determined that Agencies are responsible for determining the impact of transition on their existing C&As
  - SWG meeting of 27 April 06
- Issue 2: Agency interim authority to operate (IATO) when transitioning services provided using public telecommunications network
  - SWG determined, based on OMB policy, that an IATO would not be appropriate

Issues and Status (cont)

- Issue 3: Requirement for Government to C&A the public network
  - SWG determined that Government Agencies are not required to C&A the public Network
- Issue 4: Responsibilities of Agencies that provide contracting vehicles for telecommunications services, such as GSA
  - GSA agreed to draft a document that identifies responsibilities of contracting agencies

GSA Security Document

- Draft Developed by GSA and approved by IMC and reviewed by OMB staff
- To be signed by GSA Assistant Commissioner for ITS
- Highlights:
  - GSA will review security plans and reports in accordance with the provisions of the contract
  - GSA will monitor and resolve security issues during the life of the contract
  - GSA will conduct a Post-award C&A of contract awardees Operations Support Systems

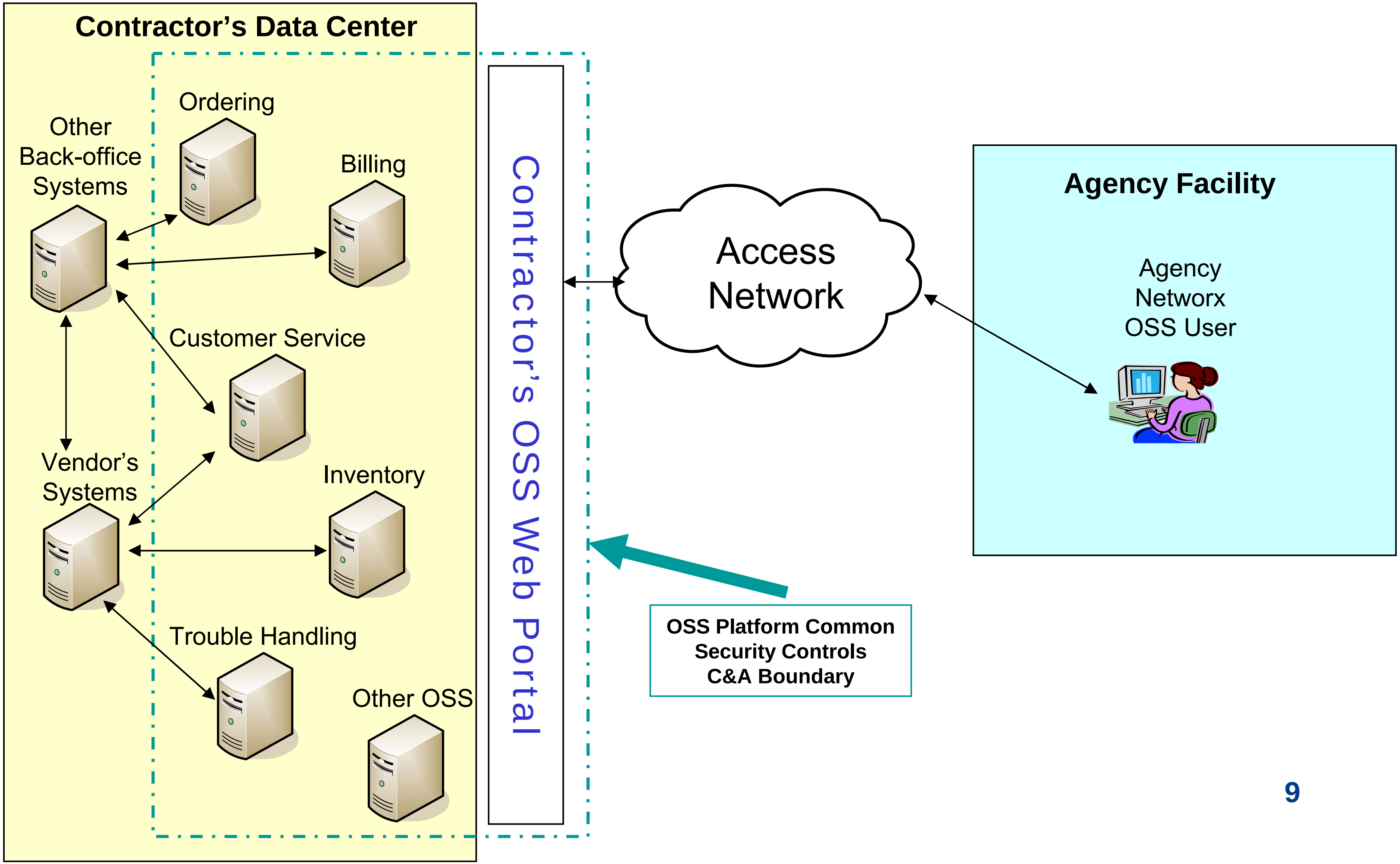
Compliance and Monitoring

- FAS OCIO will conduct C&A on GSA’s billing system
- FAS OCIO will test the full set of controls to first touch point of OSS, thereby conducting C&A of the vendor’s OSS
  - Done at security categorization = moderate impact
  - GSA will report risks to Agencies
  - Will provide continuous monitoring of OSSs per FISMA
- Agency
  - Could order additional security
  - May make a risk determination based on a GSA certification
  - May conduct its own certification
- GSA will recommend certification and accreditation of vendors OSS systems as criteria for making fair opportunity decisions

OMB A-130, Appendix III.

- "Ensure that a management official authorizes in writing, use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter.."

Networx OSS C&A Boundaries



OSS Certification

- GSA OSS Certification will be conducted by the FAS CIO
- GSA can begin the certification upon completion of NTP. Commencement of the C&A will require that the Vendor OSS is fully operational
- Certifications will be accomplished in parallel and may be accomplished in parallel with the OSS Verification testing

OSS Certification

- GSA will provide an ATO to vendors and the results of the certification to agencies for their independent determination
- GSA expects the C&A to take from 3 to 5 months from NTP to complete
- C&A’s completed for a Universal awardee who also wins an Enterprise award and uses the same OSS for both contracts will not require a second C&A for the Enterprise contract

Vendor Information Required

- Upon Notice to Proceed, awardees should be prepared to provide the following information:
  - Total Number of Systems
  - Location of Systems
  - Number of Servers
  - Type of Applications (i.e. web servers, database servers, APP Servers, etc.
  - All System boundaries/documents for each OSS to be C&A'd