



Information Security Issues

Rob McKinney



Topics

- IT Standards
- Infrastructure, Office Automation, & Telecommunications Support
 - Network Operations & Security Center
- HIPAA & FISMA



IT Standards

- **Standards Committee – advise CIO, input to ISAC**
 - **Short-term – Identify user and business needs**
 - **Define hardware and software**
 - **Support HSPD-12 effort**
 - **Standard configurations**
 - **Long-term – Define standard facilities**
 - **Meet requirements**
 - **Minimize costs**
 - **Increase efficiency**



Minimize Costs

- Bulk purchases
- Sharing IT expertise
- Reduced maintenance and implementation costs
 - Facilitates automated system use
 - Reduced training requirements
 - Reduced interoperability issues
 - Fewer configurations to support
- Leveraged Infosec efforts

Centralized C&A Group



Conduct C&A for each level



Conduct gap analysis for each facility and apply C&A for each level to all like facilities





Network Operations & Security Center (NOSC)

- WAN backbone
 - Operational support
 - Infosec support
- High value servers
 - Infosec support
- Interoperate
 - Local staffs
 - OIT
 - HHS SOCC
 - Other vendors
 - IOAT
 - ISR



Network Operations & Security Center (NOSC)

- IHS facilities
- Tribal facilities
 - Expand capabilities
 - Cost per facility description



Facility Descriptions

- Level 1 – 50- users, simple LAN with associated hubs, perhaps one or two routers or switches, possibly a firewall
- Level 2 – 50 – 200 users, a small LAN with associated hubs, routers, and or switches, possibly a firewall and servers
- Level 3 – 200 – 700 users, one or two buildings with one or two LAN's and associated hubs, routers, and switches, one or two firewalls, various servers
- Level 4 – 700+ users, one to five buildings with separate LAN's possibly a small WAN and associated hubs, routers, and switches, one or more firewalls, various servers, e.g., email, web, DNS



Estimated Costs

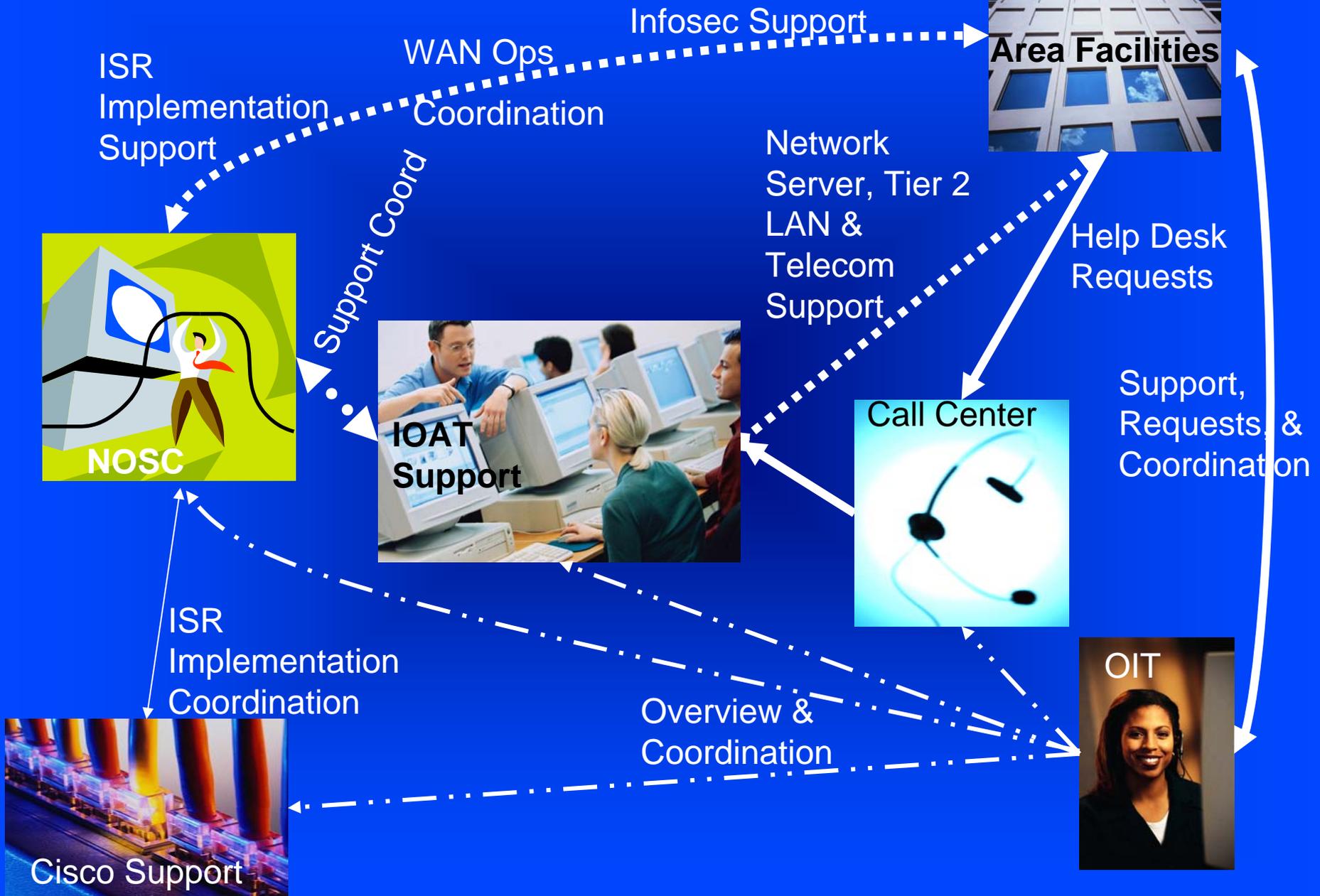
Costs	Hardware and Software (one time cost)	Labor/yr
Level 1	\$384.00	\$2,000.00
Level 2	\$960.00	\$5,000.00
Level 3	\$4,800.00	\$12,500.00
Level 4	\$13,250.00	\$15,000.00



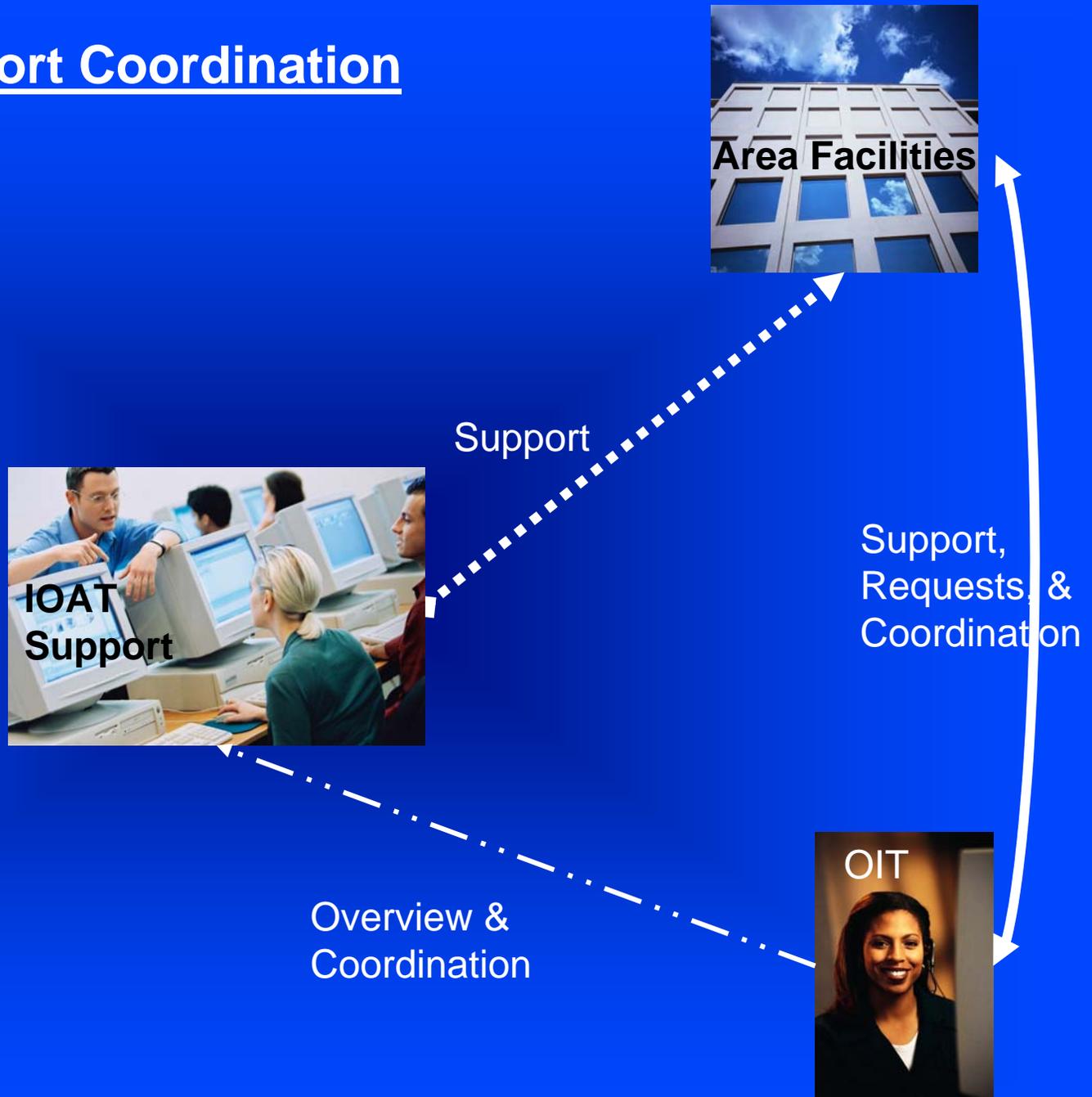
Infrastructure, Office Automation, & Telecommunications (IOAT)

- Help Desk – Tier 2
- Network service servers
 - Operational support
- Telecom support
- Interoperate
 - Local staffs
 - Other vendors
 - NOSC
 - Local WAN support

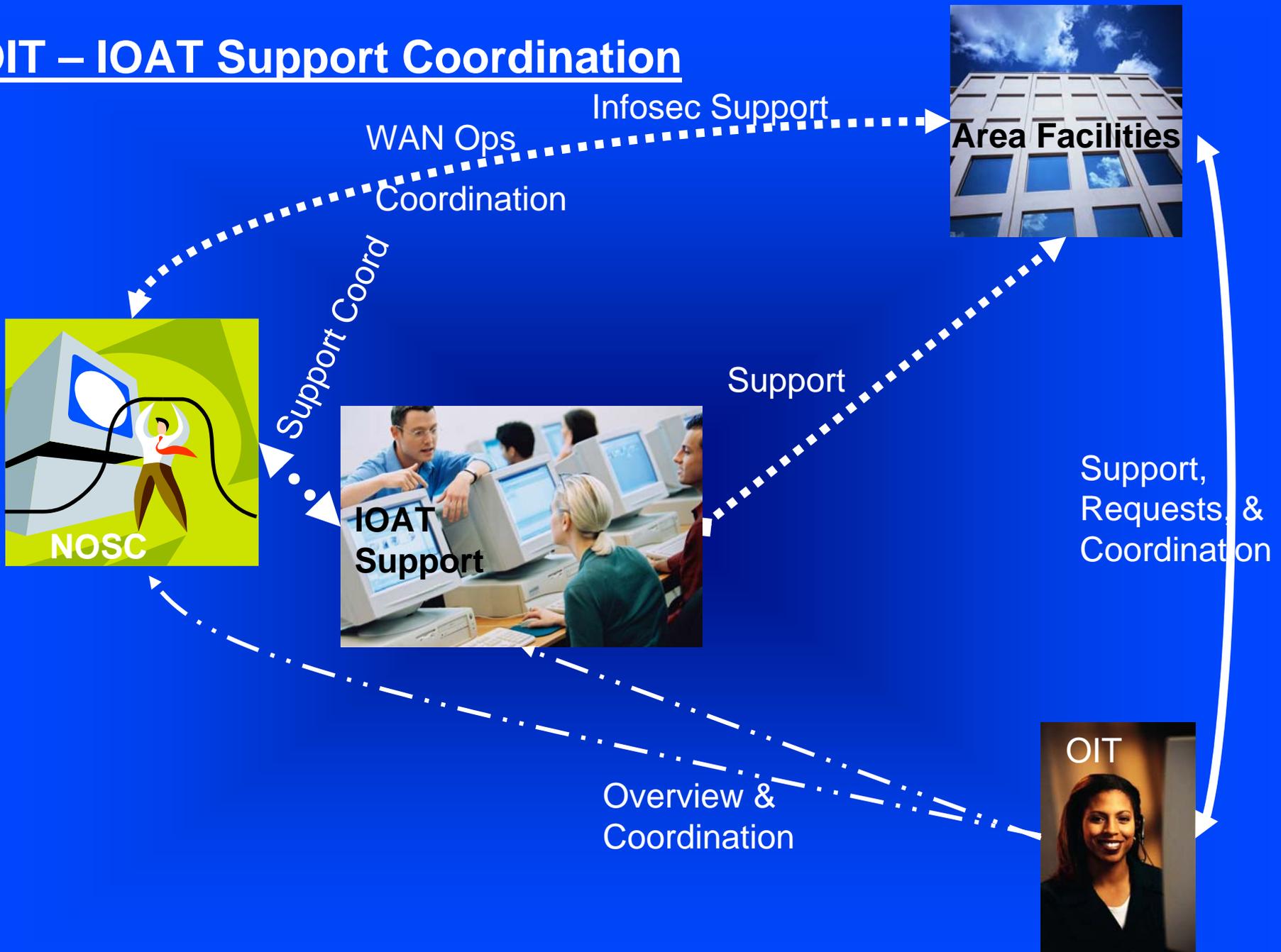
OIT – IOAT Support Coordination



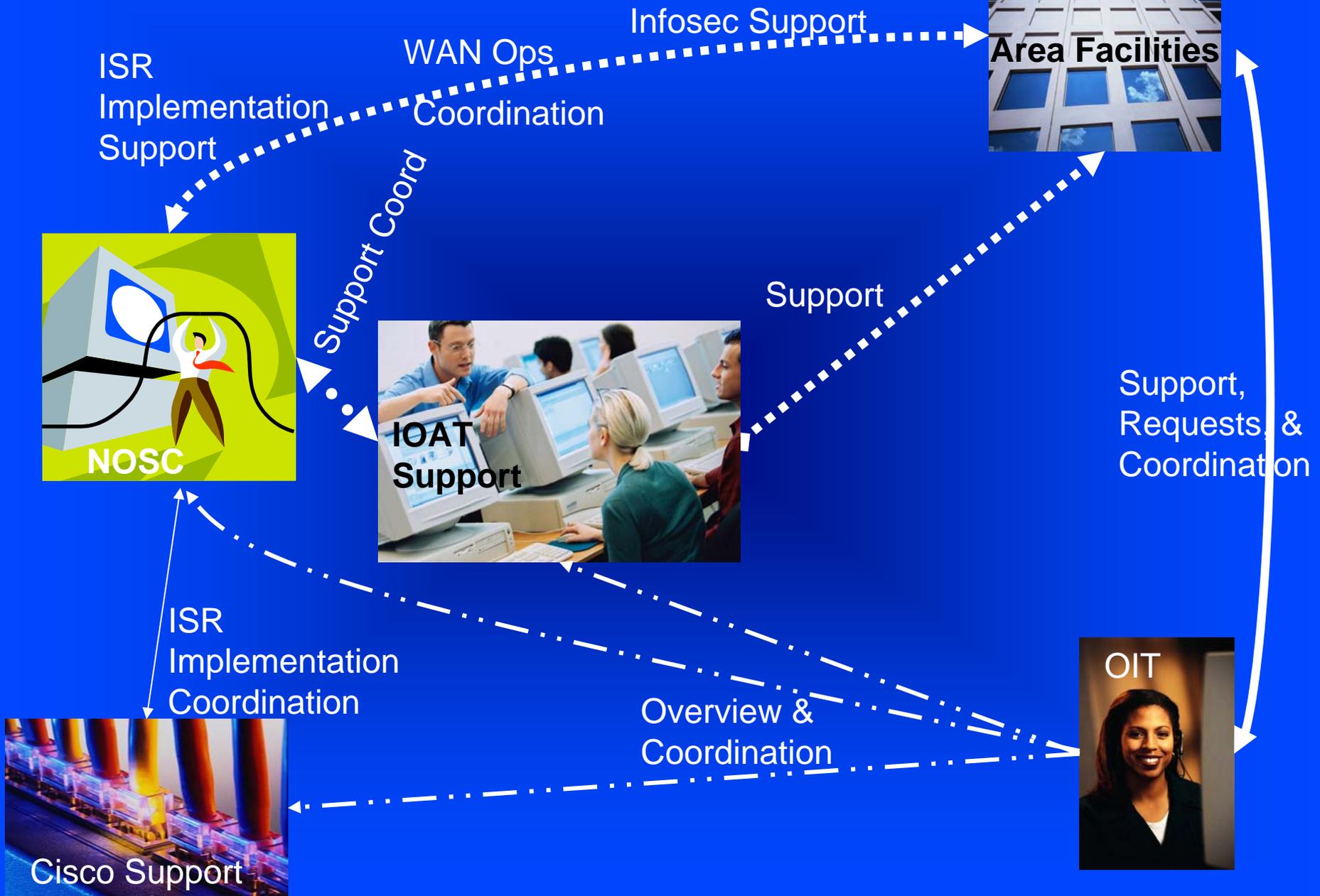
OIT – IOAT Support Coordination



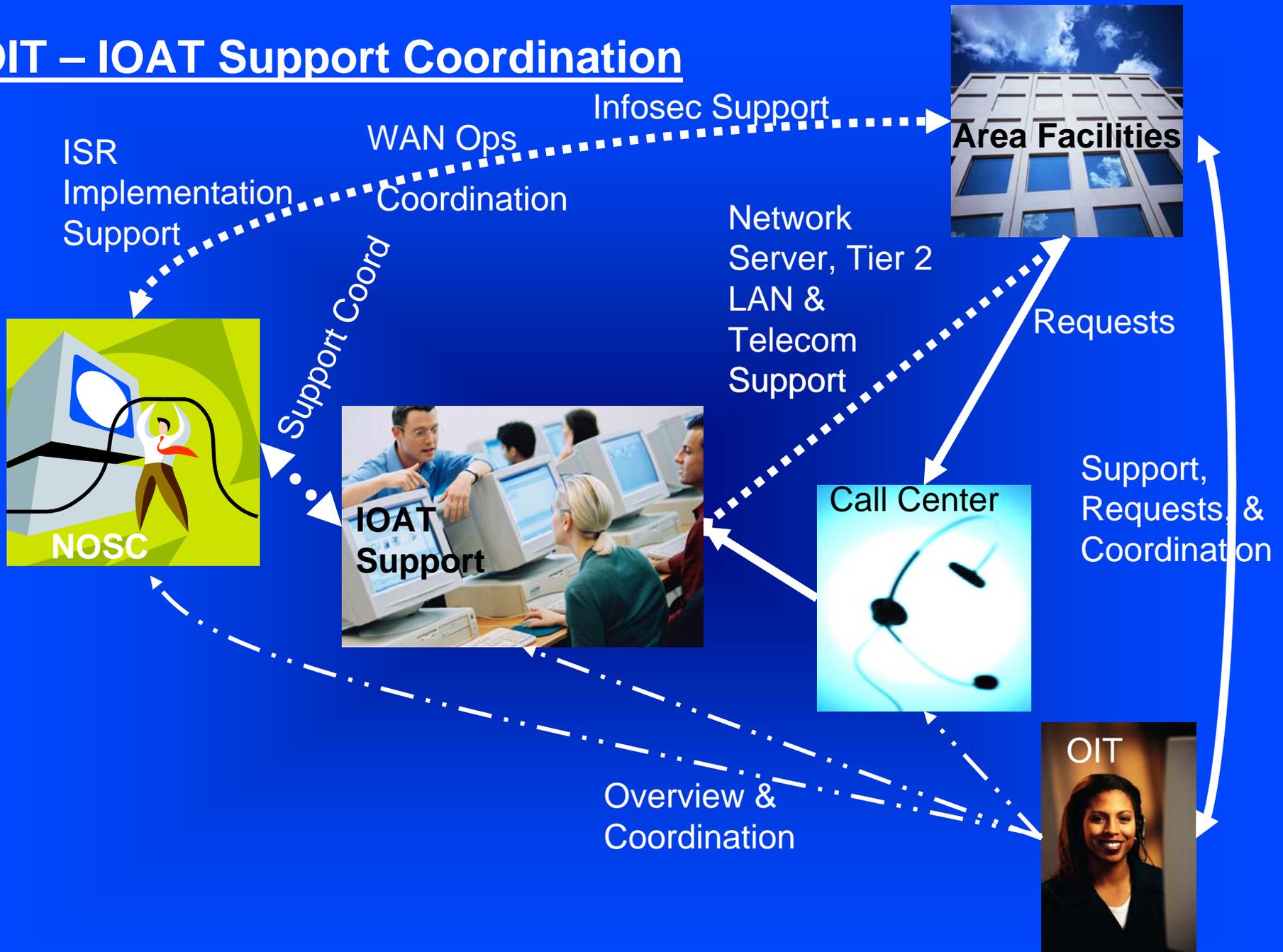
OIT – IOAT Support Coordination



OIT – IOAT Support Coordination



OIT – IOAT Support Coordination





RA In-house vs. Outsourced

- Assumptions: 386 facilities (with: 100 – level 1, 150 – level 2, 100 – level 3, and 36 – level 4);
- In-house
 - Centralized
 - Estimated total = \$5.73M + some additional costs for training, equipment etc.
 - Decentralized cost is comparable to centralized although overall costs will likely be greater due to at least some duplication of items such as tools and training
- Outsourced
 - Centralized and decentralized have the same cost estimates to accomplish RA's however, a centralized structure may be able to negotiate lower costs due to volume
 - Estimated total = \$8.4M



Minimizing Costs

- **Centralized capability**
 - Spread over three-year period
 - Provides additional services, e.g.:
 - Infosec / adhoc systems training
 - Vulnerability remediation
 - Audit
- **Use of *common information security controls* that can be applied to one or more Agency information systems**
 - Assessments of common controls can be used to support C&A's of agency information systems where those controls have been applied
 - Example: RPMS – “type” C&A
- **Possibility at the facility level:**
 - Implement standards according to representative facilities
 - Conduct C&A's on representatives and apply to others



Minimizing Costs

- **Common Infosec Controls: Facility Perspective**
 - Would require development and implementation of standards / standard infosec controls; e.g., OS's, security appliances, applications, configurations
 - Cons: some initial costs of migrating to standards, loss of some autonomy with IT systems
 - Pros: meeting standards requirement, cost reductions through bulk purchases, sharing IT expertise, reduced maintenance and implementation costs, supports move to centralized automated patch management system and NOSC, significantly reduces costs associated with C&A's, e.g., conducting 4-12 C&A's every three years vs. hundreds



HIPAA & FISMA

- Behind
- Two Areas currently undergoing risk assessments
- Five Areas have funds in the pipeline
- Documentation, training, testing
- Interconnection agreements and reviews



Summary

- **Support for standards development and implementation**
 - Develop and implement standard configurations
 - Conduct a few representative C&A's
 - Meet requirements cost effectively
 - Request SC Chairperson be on ISAC
- **Support stand up of NOSC**
 - Expansion for tribal facilities
- **HIPAA & FISMA**
 - Not compliant