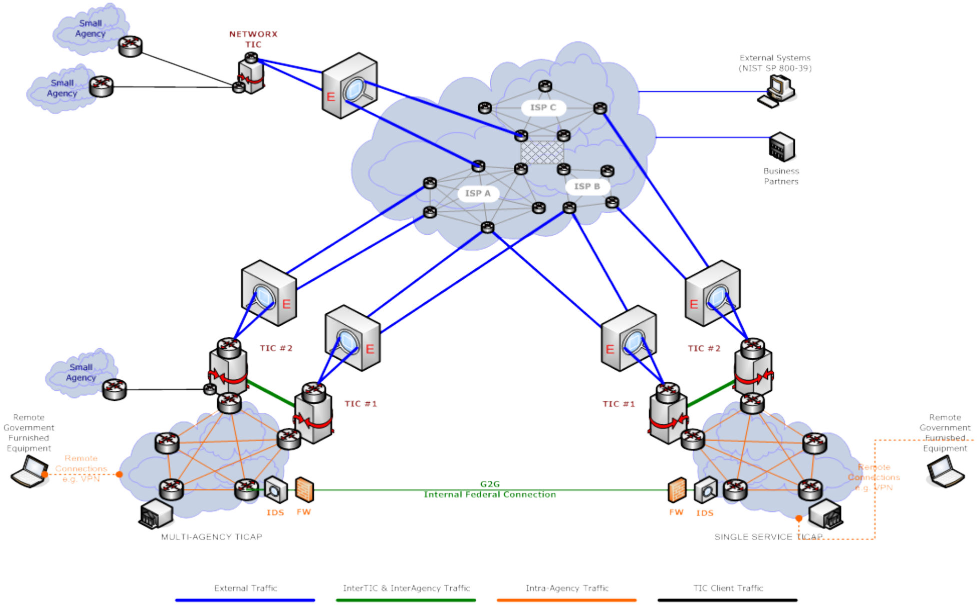
Trusted Internet Connection (TIC) Reference Architecture v2.0 Update

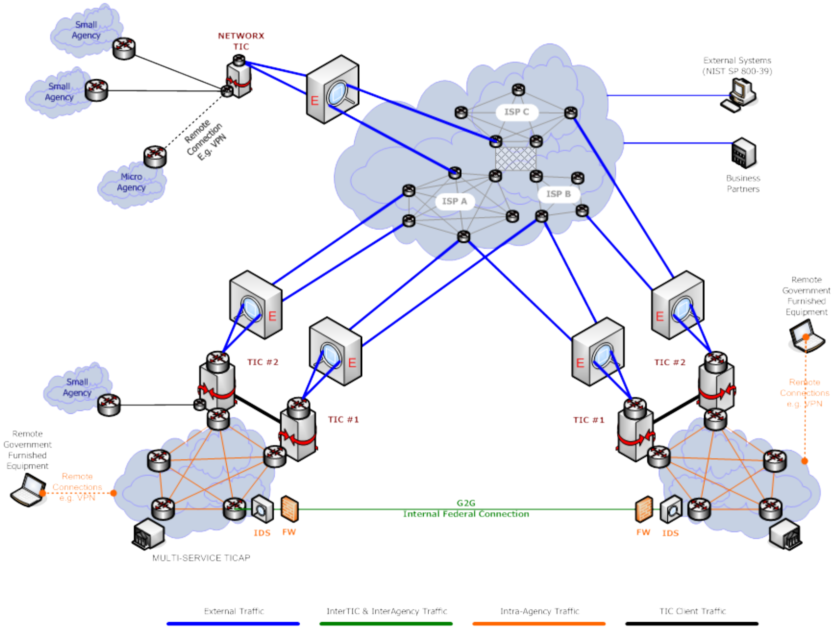
DHS Federal Network Security Branch
Sean Donelan
tic@dhs.gov

TIC Architecture Comparison

TIC 1.0


Small Agency
Small Agency
NETWORX TIC
E
ISP C
ISP A
ISP B
External Systems (NIST SP 800-39)
Business Partners
E
E
E
E
TIC #2
TIC #1
TIC #1
TIC #2
Small Agency
Remote Government Furnished Equipment
Remote Connections e.g. VPN
IDS
FW
G2G
Internal Federal Connection
FW
IDS
Remote Connections e.g. VPN
Remote Government Furnisbed Equipment
MULTI-AGENCY TICAP
SINGLE SERVICE TICAP
External Traffic
InterTIC & InterAgency Traffic
Intra-Agency Traffic
TIC Client Traffic

TIC 2.0


Small Agency
Small Agency
NETWORX TIC
Remote Connection E.g. VPN
Micro Agency
E
ISP C
ISP A
ISP B
External Systems (NIST SP 800-39)
Business Partners
Remote Government Furnished Equipment
E
E
E
E
TIC #2
TIC #1
TIC #1
TIC #2
Remote Connections e.g. VPN
Small Agency
Remote Government Furnished Equipment
Remote Connections e.g. VPN
IDS
FW
G2G
Internal Federal Connection
FW
IDS
MULTI-SERVICE TICAP
External Traffic
InterTIC & InterAgency Traffic
Intra-Agency Traffic
TIC Client Traffic

TIC 1.0 Agency Comments Addressed

1. TIC policies
   - What data/information can be exempt from TIC?
   - TIC capabilities written as questions, what do they mean?
   - Did not specify any security policies for the TIC
2. Design Concepts
   - Facilities & personnel requirements should more appropriately match mission
   - Clarification of TIC concepts and relationships between TIC objects
3. Clarified Language and Intent based on evolving environment
   - TICAPs must meet other Federal/OMB policies
   - New capabilities needed
4. Technical Clarification and Security Gaps
   - Access by staff outside the continental United States, concern about backhaul problems
   - Clarify the examples for ‘internal’ and ‘external’ remote access connections
   - Clarify TIC requirements for VPNs with Trusted business partners

1. TIC Policies

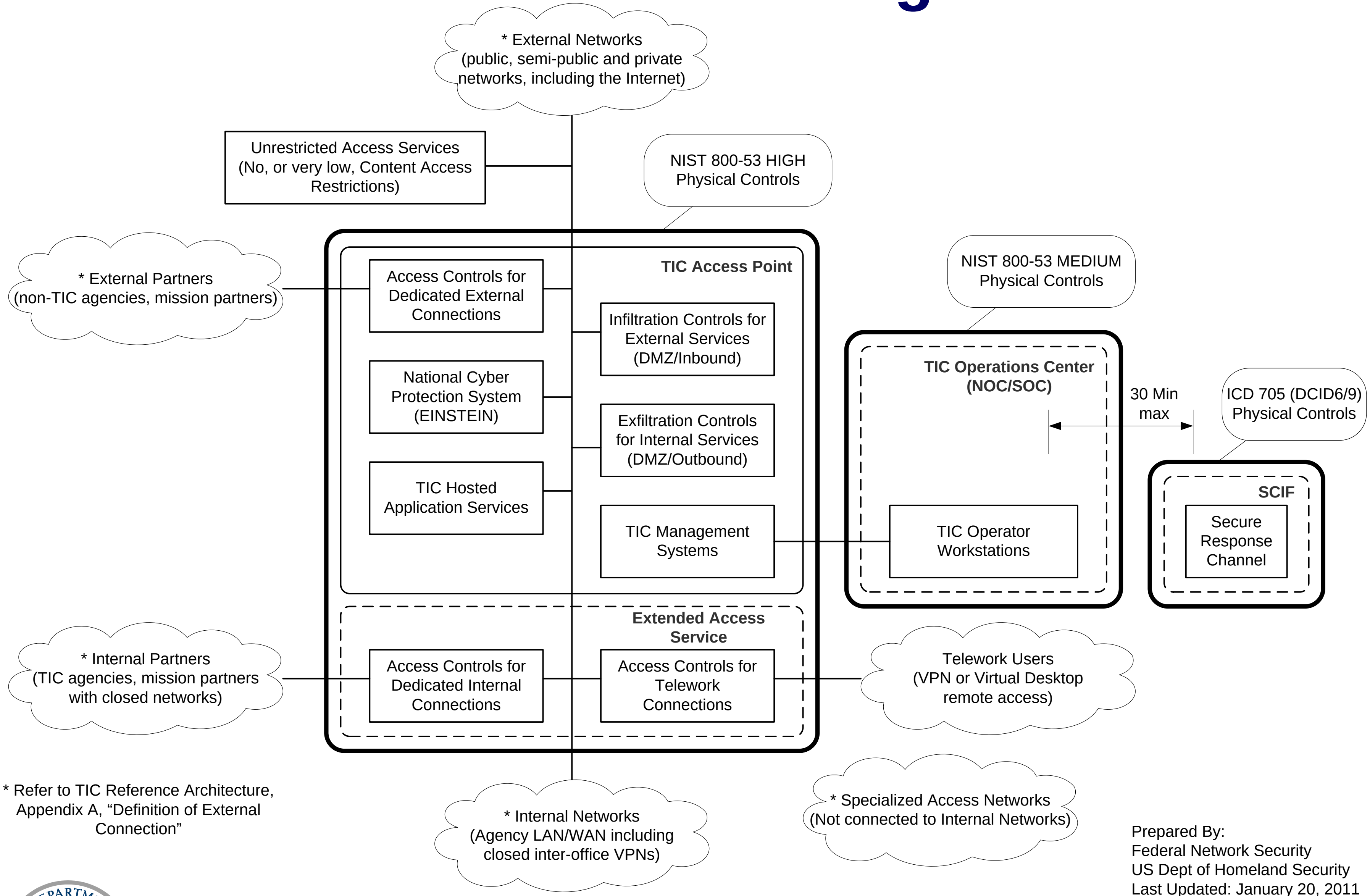
- Added definition for “unrestricted” data
  - Unrestricted access data has no legal or other restrictions on access or usage and may be open to the general public
  - Example: www.whitehouse.gov outside of TIC
- Established security policies
  - Default deny, permit by exception
  - Source egress IP address filtering
  - FedRelay (Deaf/Hard of Hearing Support)

2. Design Concepts

Organized TIC components into functional blocks with different requirements

- TIC access points
  - FIPS 199 for high impact systems (Physical)
- TIC management locations (NOC/SOC)
  - FIPS 199 for medium impact systems (Physical)
- Sensitive Compartment Information Facility (SCIF)
  - DCID 6/9 Physical Security Standards (Physical)

TIC 2.0 Functional Block Organization



* External Networks
(public, semi-public and private networks, including the Internet)

Unrestricted Access Services
(No, or very low, Content Access Restrictions)

NIST 800-53 HIGH
Physical Controls

* External Partners
(non-TIC agencies, mission partners)

TIC Access Point

Access Controls for Dedicated External Connections

Infiltration Controls for External Services (DMZ/Inbound)

National Cyber Protection System (EINSTEIN)

Exfiltration Controls for Internal Services (DMZ/Outbound)

TIC Hosted Application Services

TIC Management Systems

NIST 800-53 MEDIUM
Physical Controls

TIC Operations Center (NOC/SOC)

TIC Operator Workstations

30 Min max

ICD 705 (DCID6/9)
Physical Controls

SCIF

Secure Response Channel

Extended Access Service

* Internal Partners
(TIC agencies, mission partners with closed networks)

Access Controls for Dedicated Internal Connections

Access Controls for Telework Connections

Telework Users
(VPN or Virtual Desktop remote access)

* Specialized Access Networks
(Not connected to Internal Networks)

* Internal Networks
(Agency LAN/WAN including closed inter-office VPNs)

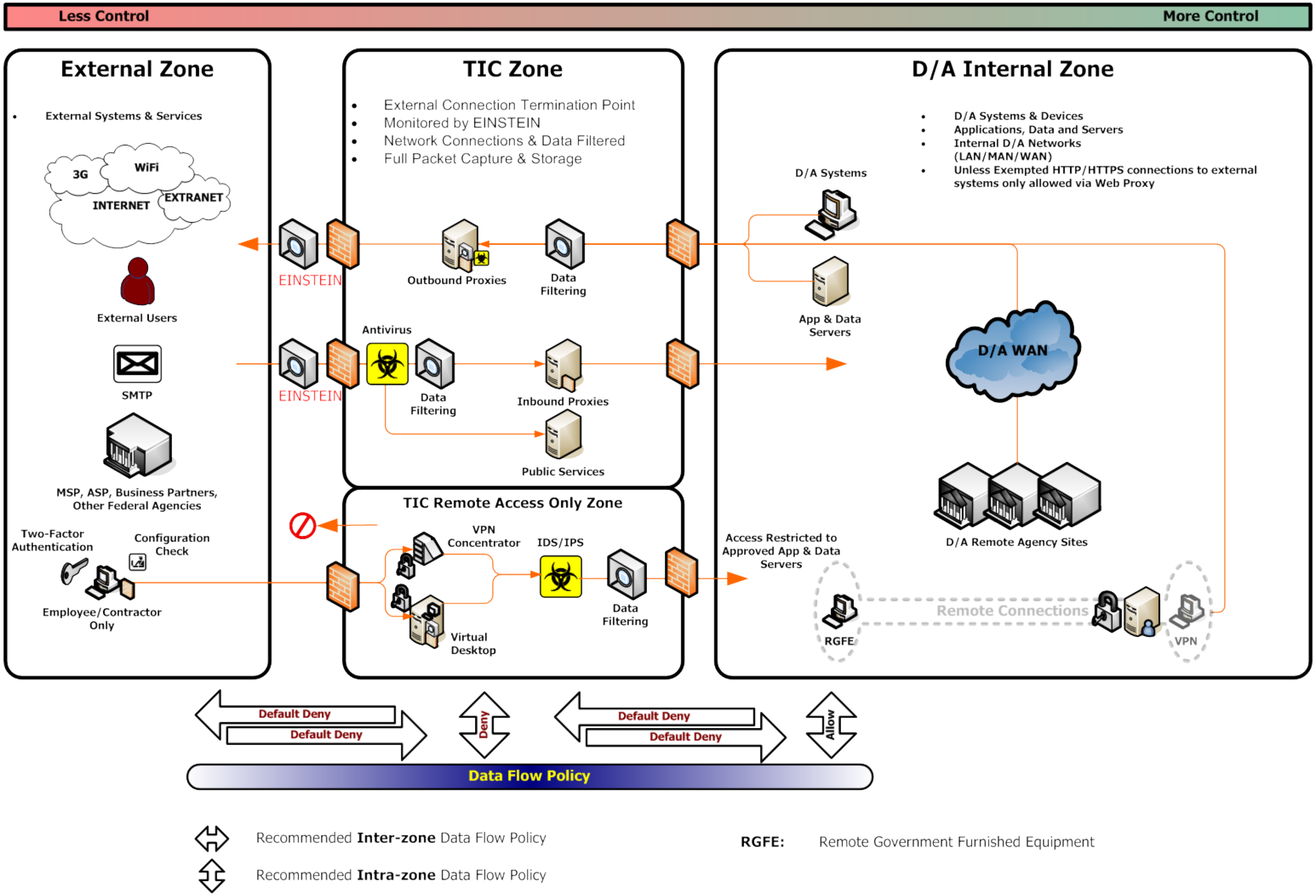
* Refer to TIC Reference Architecture, Appendix A, “Definition of External Connection”

Prepared By:
Federal Network Security
US Dept of Homeland Security
Last Updated: January 20, 2011

3. Clarified Language and Intent

- TICAPs need to meet other Federal/OMB policies
  - DNSSEC, IPv6, HSPD-12, NSTIC, incident reporting
- TICAP minimizes use of cleartext management protocols
- TICAP routing protocol authentication (BGP security)
- Expand VPN/Remote access alternatives
- E-Mail forgery detection / Sender authentication
- DNS query filtering
- Data leak prevention policy documentation
- Network inventory process
- Operational exercise participation
- Vulnerability scanning, continuous monitoring

4. Technical Clarification and Security Gaps



Less Control

More Control

External Zone

- External Systems & Services

TIC Zone

- External Connection Termination Point
- Monitored by EINSTEIN
- Network Connections & Data Filtered
- Full Packet Capture & Storage

TIC Remote Access Only Zone

D/A Internal Zone

- D/A Systems & Devices
- Applications, Data and Servers
- Internal D/A Networks (LAN/MAN/WAN)
- Unless Exempted HTTP/HTTPS connections to external systems only allowed via Web Proxy

Data Flow Policy

⇔ Recommended **Inter-zone** Data Flow Policy

⇕ Recommended **Intra-zone** Data Flow Policy

RGFE: Remote Government Furnished Equipment

TIC Compliance Validation Scoring

- FY11 Assessments planned
  - All 19 TICAPs
  - All 4 MTIPS vendors
  - 8 seeking Service Agencies
- Scoring Criteria
  - TIC 1.0 Capabilities are the standard
  - Unofficially scored on the TIC 2.0 Capabilities
  - A few agencies prefer scoring only on TIC 2.0
- Additional Assessments
  - Risk & Vulnerability Assessments (RVA)
  - Network Mapping and Baselining (NMB)
  - Cybersecurity Alert & Remediation Tracking (CART)
  - Automated Validation Tools

Selected TIC 2.0 Implementation Milestones

- ✓ TIC Interagency Work Group meeting
- ✓ MTIPS vendor meetings
- ✓ Stakeholder review of the TIC Architecture v2
- ✓ DHS review and approval of TIC Architecture v2
- ✓ Develop TCV scoring criteria by Q2 FY11
- □ Publish Memo with TIC 2.0 guidance by Q2 FY11
- □ Begin scoring using TIC 2.0 by Q2 FY11
- □ GSA and the MTIPS contract modification by Q2 FY12
- □ All TICAPs/MTIPS upgrade to TIC 2.0 by Q4 FY12
- □ Ongoing activities include:
  - FNS Website and OMB MAX Portal
  - Public affairs guidance and outreach
  - Coordinate Interagency meetings and data calls
  - Support of GSA and MTIPS vendors

Homeland
Security