From: ACT/IAC IPv6 Project Plan Team
- Atacan Donmez, Converge Network Corp.
- David Harris, SAIC
- William Kyburz, GDIT, Lead
- Jennifer Tomlin, SAIC
- Ralph Wallace, Command-Control, LLC

Date: March 22, 2011

To: Chris Chroniger, ACT/IAC IPv6 Task Force, and Government IPv6 Task Force

The ACT/IAC Project Plan Team is pleased to present the attached Work Breakout Structure (WBS) for the Government's consideration and use for IPv6 project planning. The WBS covers project activities from creation of the Transition Plan through the Pilot and Production phases.

Several notes on the WBS:

1. We kept the WBS at the respective level (3) in order to provide broad guidance and not go deeper which could be construed as constraining compliance or governance.
    a. Should the task force wish the WBS be refined and lower tiers inserted, we can easily support this.
2. WBS element 1.1.2 refers parenthetically to a "workflow". If desired, Ralph Wallace can provide this workflow as a "representative" element of the transition planning process from industry best practices. The workflow serves a double purpose; one for transition planning information discovery, and the other for change management key stakeholder buy-in.
3. In WBS element 1.2 there is a reference to "SMART" criteria, which stands for **S**pecific, **M**easurable, **A**chievable, **R**ealistic and **T**imely.
4. Although a "Schedule Phase" field is provided in the spreadsheet, no dates are provided in this version since each utilizing Government Department/Agency may already be working against their own internal schedule or have varying degrees of implementation complexity and/or resource availability. Should the Task Force desire, we can provide a notional suggested timeline.
5. In section 6.1, "Segment 1+n (per workflow)" refers to a network segment. Although, the WBS did not include a prioritizing task, we recommend that segments be prioritized based on criteria useful to the specific Government Department, such as unclassified systems first, then Secret systems, then Top Secret systems or other organizational criteria such as budget, users, sensitivity, complexity, partner activities, etc.

A special thanks goes to Ralph Wallace for his initial creation of the baseline WBS and David Harris for his review.

Task	Schedule Phase
1. Create Transition Plan	**Plan**
1.1. Assess Enterprise Architecture state of readiness	
1.1.1. Request Documentation	
1.1.2. Conduct "As Is" Assessment (per Workflow)	
1.2. Develop “To Be” Architecture Goals per SMART criteria	
1.3. Scope Transition Project	
1.3.1. Establish overarching system development life cycle (SDLC)	
1.4. Create and Staff Transition Project Plan	
1.5. Implement Transition Project Plan	
2. Plan the Transition	**Plan**
2.1. Establish Transition PMO	
2.1.1. Establish governance organization, processes and reporting structure	
2.1.2. Establish schedule milestones per the SDLC (Requirements, Design, Test, Pilot, Production)	
2.2. Communication and Training Plan Development (Change Management)	
2.2.1. Implement Communications and Training Plan for all identified stakeholders	
2.2.1.1. Internal IPv6 Seminars	
2.2.1.2. Implementing IPv6	
2.2.1.3. Securing IPv6	
2.2.1.4. IPv6 for the Service Desk (Tiers 1,2,3)	**Pilot (3.8), Production (4.1.4)**
2.2.1.5. IPv6 for the Computer Incident Response Team	**Pilot (3.8), Production (4.1.4)**
2.3. Acquisition Policy Development (IAW NIST and FAR)	
2.4. Security Policy Development and Engineering Planning	
2.5. Risk Mitigation Planning	
2.5.1. Transition retreat plan	
2.5.2. Non-IPv6 Capable Infrastructure mitigation	
2.6. Address Allocation and Management Planning	
2.7. Network Architecture Development	
2.7.1. Establish IPv6 connectivity criteria	
2.7.2. Develop IPv6-Ready Matrix of Enterprise’s IT Infrastructure & Applications	
2.7.3. Develop High-Level Architecture System and Technical Views	
2.8. Infrastructure Integration Planning	

Task	Schedule Phase
2.8.1. Cyber Security Infrastructure	
2.8.2. Router	
2.8.3. Server	
2.8.4. Desktop	
2.9. Application Planning	
2.10. Test Planning	
2.11. Pilot Strategy Planning	
2.11.1. Critical Success Factors	
2.11.2. Test Planning	
2.12. Create and Staff Transition Plan	
2.13. Implement Transition Plan	
3. Test Lab Operations	**Pilot**
3.1. Establish Test Workflow and Governance	
3.2. Establish Performance Metrics - Network and Apps	
3.3. Network connections (ISP, routers, remote access)	
3.4. Network Infrastructure (DNS, DHCPv6)	
3.5. Security Development	
3.5.1. Firewall	
3.5.2. IDS/IPS	
3.5.3. Authentication Services (IPSec, SSL)	
3.5.4. Remote Access	
3.5.5. Deep Packet Inspection	
3.6. Platform Pilot	
3.6.1. Server	
3.6.2. Desktop/Laptop	
3.6.3. Network Management Tools	
3.7. Applications Build Pilot	
3.7.1. Common User Apps	
3.7.2. Enterprise Applications (including GOTS IPv4 Apps.)	
3.7.3. Application IPv4 & IPv6 Synchronization	
3.8. Test	
3.8.1. Test Case per Critical Success Factor, Risk Matrix, and NIST guidelines	
3.82. DIACAP or FISMA Security C&A	

Task	Schedule Phase
3.9. Review and Document	
3.9.1. Conduct After Action Review	
3.9.2. Document Architecture	
3.9.3. Document Operations Best Practices	
3.9.4. Document Security Best Practices	
3.9.5. Develop Help-Desk/CIRT Documentation	
3.9.6. Compile Lessons Learned	
3.9.7. Update training from Lessons Learned and conduct training	
3.9.8. Update Transition Plan with Test Results Lessons Learned	
4. Production Pilot	**Production**
4.1. Prep IT Support	
4.1.1. Establish deployment workflow and governance	
4.1.2. Develop help desk procedures	
4.1.3. Develop CIRT procedures	
4.1.4. Train on pilot infrastructure	
4.2. Security Deployment	
4.2.1. Firewall	
4.2.2. IDS	
4.2.3. Authentication Services	
4.2.4. Remote Access	
4.2.5. Deep Packet Inspection	
4.3. Network connections	
4.3.1. ISP Service	
4.3.2. Internal Routers & Switches	
4.3.3. Remote Access Service	
4.4. Network Infrastructure	
4.4.1. DNS	
4.4.2. DHCPv6	
4.4.3. Network Management Tools	
4.5. Platform Deployment	
4.5.1. Server	
4.5.2. Desktop	
4.6. Enterprise Applications (including GOTS IPv4 apps.)	

Task	Schedule Phase
4.6.1. Application IPv4 & IPv6 Synchronization	
4.7. Test	
4.7.1. Test Case per Critical Success Factor, Risk Matrix, and NIST guidelines	
4.7.2. DIACAP or FISMA Security C&A	
4.8. Review and Document	
4.8.1. Conduct After Action Review	
4.8.2. Update Architecture Documents	
4.8.3. Update Operations Best Practices (refine workflow)	
4.8.4. Update Security Best Practices (refine workflow)	
4.8.5. Update Help-Desk Procedures	
4.8.6. Update CIRT Procedures	
5. Enterprise Deployment (Initial)	**Production**
5.1. Segment 1 (per workflow)	
5.1.1. System Infrastructure 1 (Servers, Desktops, Laptops, PDAs)	
5.1.2. Network Fabric 1 (Switches, Routers, Gateways, DHCP, DNS)	
5.1.3. Cyber Security 1 (Firewalls, IDS/IPS, Scanner (Einstein/Retina))	
5.1.4. Application 1 (Business, Mission)	
5.2. Review and Document	
5.2.1. Conduct After Action Review	
5.2.2. Document Architecture	
5.2.3. Document Operations Best Practices	
5.2.4. Document Security Best Practices	
5.2.5. Refine Help-Desk/CIRT Documentation	
5.2.6. Compile Lessons Learned	
5.2.7. Update training from Lessons Learned and conduct training	
6. Enterprise Deployment (On-Going)	**Production**
6.1. Segment 1+n (per workflow)	
6.1.1. System Infrastructure 1+n (Servers, Desktops, Laptops, PDAs)	
6.1.2. Network Fabric 1+n (Switches, Routers, Gateways, DHCP, DNS)	
6.1.3. Cyber Security 1+n (Firewalls, IDS/IPS, Scanner (Einstein/Retina))	
6.1.4. Application 1+n (Business, Mission)	
6.2. Review and Document (per n installation)	

Task	Schedule Phase
6.2.1. Conduct After Action Review	
6.2.2. Document Architecture	
6.2.3. Document Operations Best Practices	
6.2.4. Document Security Best Practices	
6.2.5. Refine Help-Desk/CIRT Documentation	
6.2.6. Compile Lessons Learned	
6.2.7. Update training from Lessons Learned and conduct training	