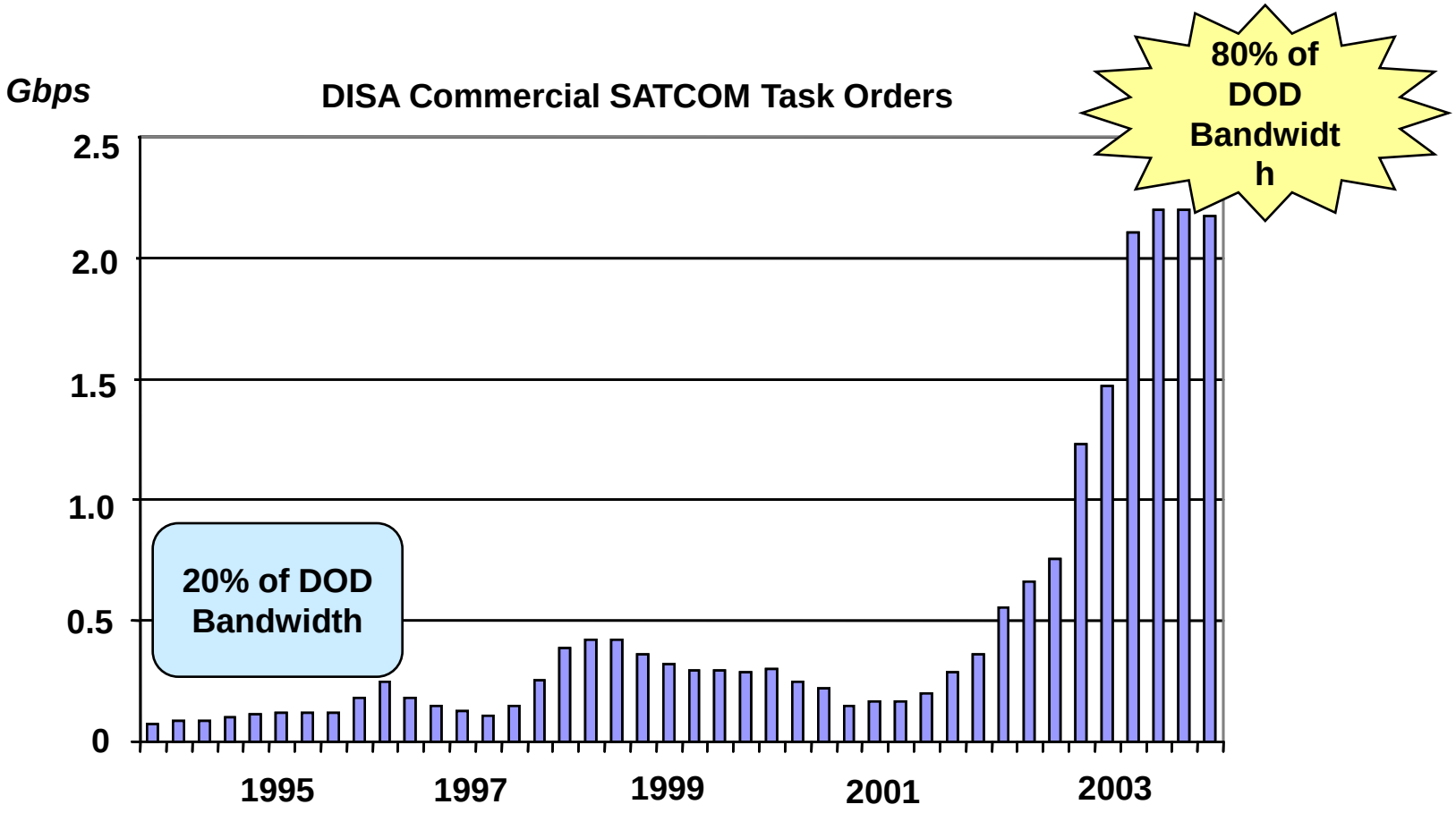
National Security Space Office

Commercial SATCOM Protection Performance Criteria

Richard H. Buenneke
National Security Space Engineering
The Aerospace Corporation
Arlington, Va.
richard.buenneke.ctr@osd.mil

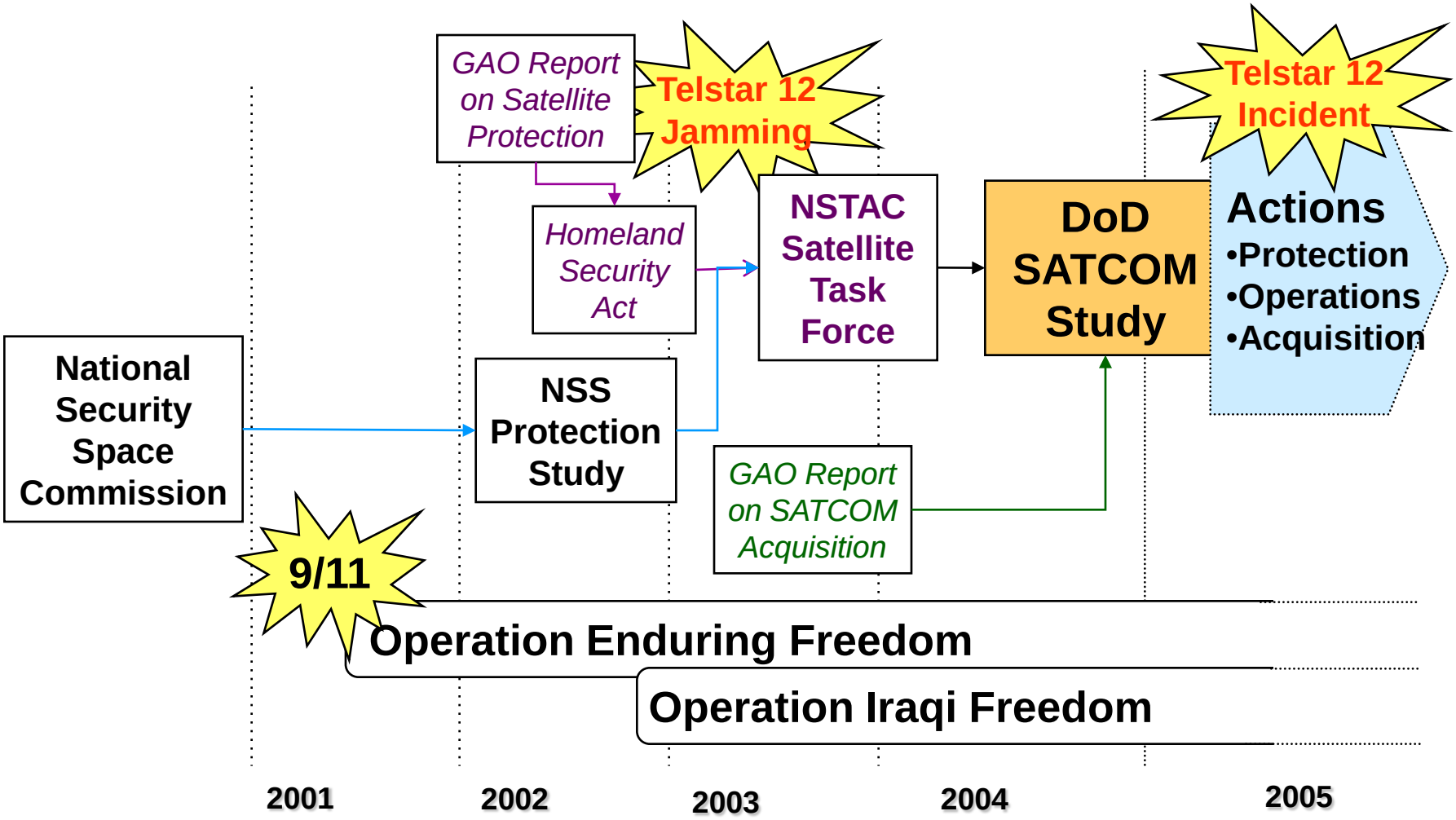
13 Dec 2005

DoD Commercial SATCOM Usage



Note: Requirements from NRO, NGA, and NSA are not included

Study Context



DoD Commercial SATCOM Study

- Conducted from March 2004-March 2005, under sponsorship of:
  - Undersecretary of the Air Force/DoD Executive Agent for Space
  - Commander, U.S. Strategic Command
  - Assistant Secretary of Defense (Networks & Information Integration)
- Deliverables
  - ASD(NII) -- Revised DoD Commercial SATCOM Fixed Satellite Services policy
  - NSSO and USSTRATCOM --Criteria for protection and operational management based upon commercial “best practices”

Protection Working Group Survey

- Survey expands upon general vulnerability analysis by NSTAC Satellite Task Force
  - Company-specific surveys and site visits
  - Definition of protection “best practices” for incorporation into new DoD acquisition strategy
- Survey recommendations also address key implementation issues
  - Coordination on “purposeful interference” preparedness and response with DoD and other federal agencies:
    - Department of Homeland Security
    - Federal Communications Commission
    - Department of State
    - Intelligence Community
  - National Security Agency approval of commercial space information assurance solutions

Industry Participants

- Global FSS operators
  - Eutelsat
  - Intelsat
  - New Skies
  - PanAmSat
  - SES Americom
- DISN Satellite Transmission Services Global (DSTS-G) contractors
  - Arrowhead
  - Artel
  - Spacelink
- Global MSS operators
  - Inmarsat

Protection Criteria

- Information sharing and analysis
- Situational awareness
  - RFI and incident reporting
  - Space traffic management
  - Network disruption reporting
- Global Network Operations
  - Operations management
  - Cyber/network security
  - Operations security
- TT&C information assurance
- Terrestrial physical security
- Supporting infrastructures
- Personnel security

Protected Commercial SATCOM for National Security

Capability and Effect

Protection Performance Criteria

Bonus	• Exceptional performance
Objective	• Sustains or extends current best practice • Basis for contract award fees
Threshold	• Derived from current best practice • Basis for supplier selection decisions
Unsatisfactory	• Shortfall from prevailing commercial practice • Upgrade to threshold level should occur as soon as practicable

Information Sharing and Analysis

Bonus	• Secure, automated incident reporting at primary and backup satellite and network operations centers
Objective	• Information sharing on company-specific susceptibilities • Participation in DHS and DoD-sponsored threat and vulnerability assessments
Threshold	• Membership in (or affiliation with) DHS's Telecommunications Information Sharing and Analysis Center • NIAP-approved COMSEC at operations centers
Unsatisfactory	• No participation in sector-coordinating mechanism • No secure communications capability

EMI/RFI Incident Management

Bonus	• Participation in DoD and DHS combined multi-threat response exercises
Objective	• Support in development of USSTRATCOM tactics, techniques and procedures
Threshold	• Access to commercial SATCOM RFI geolocation capabilities • Documented processes for identification, reporting and resolution of EMI/RFI • Participation in DoD-sponsored EMI/RFI exercises • SECRET security clearances for key operations staff involved in DoD-sponsored EMI/RFI exercises and operational management
Unsatisfactory	• No documented processes for intentional RFI incidents

Situational Awareness

Bonus	• Participation in Air Force space situational awareness planning and concept of operations (CONOPS) development
Objective	• Use of AFSPC space surveillance network data for space traffic management • Participation in joint DoD-DHS SSA data fusion demonstrations
Threshold	• Documented processes for station keeping and major satellite maneuvers • Routine operator reporting of satellite position information and major maneuvers • Reporting of major disruptions to DoD networks
Unsatisfactory	• No documented procedures for station keeping and satellite maneuvers

Operations Management

Bonus	• Participation in USSTRATCOM Joint Task Force-Global Network Operations planning and exercises
Objective	• Direct connection of service provider's network operations center to Commercial SATCOM System Expert and USSTRATCOM • End-to-end fault and performance management • Mutual aid agreements with other satellite operators
Threshold	• Coordinated spectrum monitoring • Support to USSTRATCOM and DISA fault and performance management process reengineerings
Unsatisfactory	• No coordination of spectrum monitoring • Fragmented performance management

Cyber Security

Bonus	•Operating system diversity to minimize exposure to Windows Operating System vulnerabilities. •Robust back-up (full capability)
Objective	• Intrusion detection systems • Vendor-diverse firewall/proxy servers (defense in-depth)
Threshold	• Annual risk audits by certified external organization • Anti-virus and worm detection software installed on all systems. • Documented operational procedures • Perimeter firewalls
Unsatisfactory	• Minimal system protection with insufficient monitoring

Terrestrial Network

Bonus	• Complete air-gap separation of mission critical systems associated with Mission Assurance Category I user traffic • Fully capable backup network operations center and available operations staff
Objective	• Periodic network mapping and penetration testing by independent third-party • Dual comm paths for alarms and emergency management • Limit external connectivity to network operations center via virtual private networks. • No direct connectivity to spacecraft and payload operations centers from external networks
Threshold	• Physically path diverse connectivity, service provision by multiple telecom providers where available. • Carefully managed internal connectivity paths
Unsatisfactory	• Non-compliance with threshold levels

Operations Security

Bonus	• Participation in development of OPSEC planning guidance
Objective	• Minimization of OPSEC indicators during exercises and EMI/RFI response activities
Threshold	• Specific information on military unit identities and locations for DoD networks limited to SECRET-cleared staff • External connectivity for DoD provisioning and customer care data limited to VPNs • NSA-approved COMSEC at all operations centers • Employee-awareness training program on OPSEC information
Unsatisfactory	• Minimal protection of OPSEC indicators • Minimal protection of provisioning and customer care data

TT&C Information Assurance

Bonus	• NSA-approved telemetry, tracking and command encryption and authentication employed on all satellites carrying Mission Assurance Category I, II and III information
Objective	• NSA-approved command encryption and authentication solution employed on all satellites carrying MAC I and II information
Threshold	• NSA-approved command authentication solution on spacecraft carrying MAC I and II information
Unsatisfactory	• No command authentication or encryption on satellites carrying national security information

Terrestrial Physical Security

Bonus	• Participation in national, state and local preparedness exercises • Integration of business continuity exercises with DoD operational exercises
Objective	• Analyses of interdependencies with other infrastructures • Collaboration with neighboring private sector owners of critical infrastructures and key assets
Threshold	• Annual independent audits of physical security plans • Biennial, comprehensive crisis management exercises • Collaboration with state and local public safety authorities
Unsatisfactory	• No independent assessments of physical security plans • Tabletop business continuity exercises

Supporting Infrastructures

Bonus	• Participation in multi-sector interdependency analyses • Participation in multi-sector preparedness exercises
Objective	• Exercises using back-up power sources • Priority for consumables resupply and service restoration
Threshold	• Regular tests of uninterruptible power source and back-up generators • Documented consumable management and re-supply plan
Unsatisfactory	• No regular testing of backup sources • No documented processes for restoration of services

Personnel Security

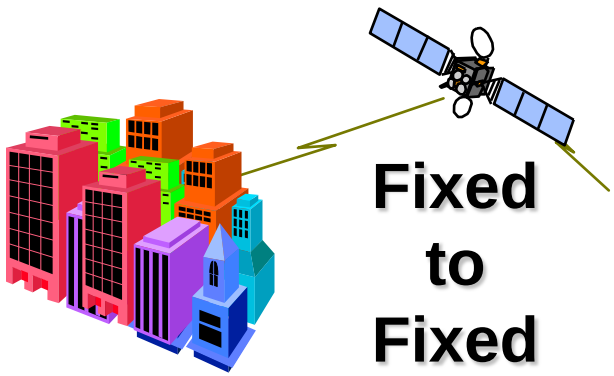
Bonus	• National SECRET clearances for key company officers
Objective	• Periodic re-checks with national authorities for operations staff
Threshold	• Background checks with local law enforcement and national authorities for operations staff • U.S. SECRET clearances for all personnel in direct contact with sensitive DoD OPSEC indicators
Unsatisfactory	• No background checks • Checks of references designated by applicant

Follow-on activities

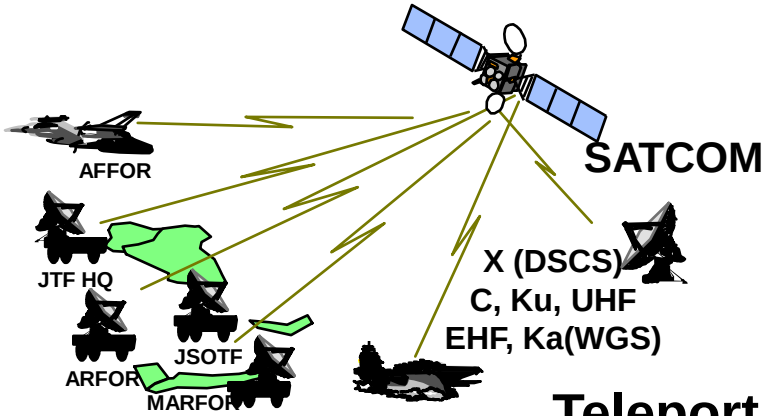
- Joint Staff –Lead Network Centric Function Capabilities Board review of protection and other “floor” requirements
- DISA – Revise acquisition strategy to accommodate new warfighter requirements
- USSTRATCOM – Develop and refine operational and functional plans
- NSSO – Facilitate DoD-industry dialogue on protection and preparedness

Back Ups

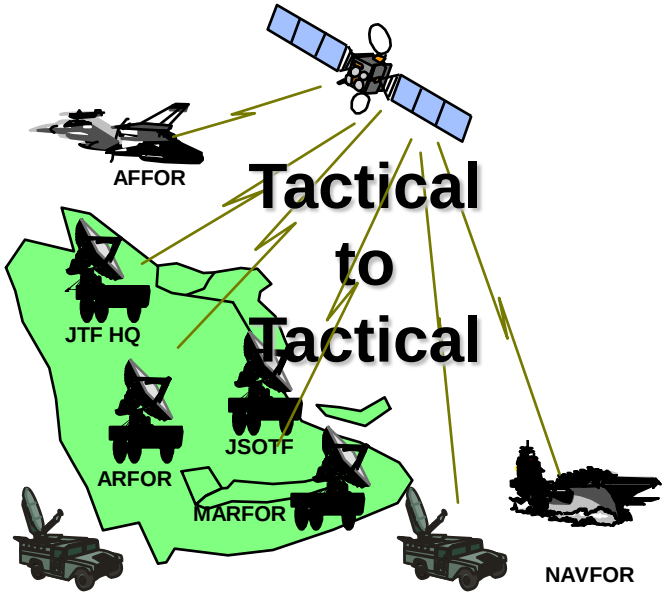
Types of COMMSATCOM Services



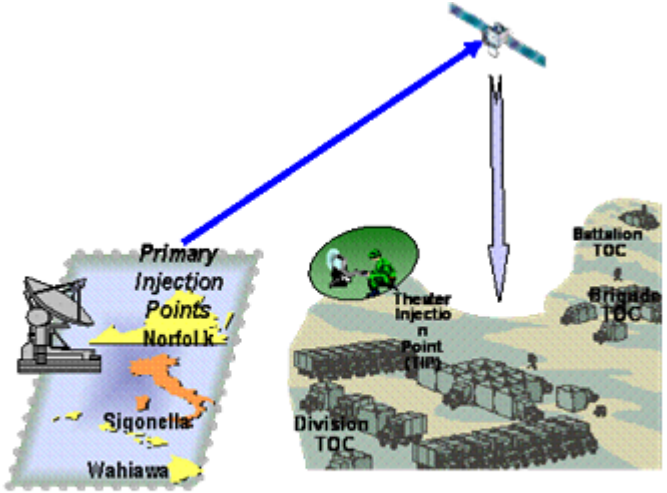
Fixed
to
Fixed



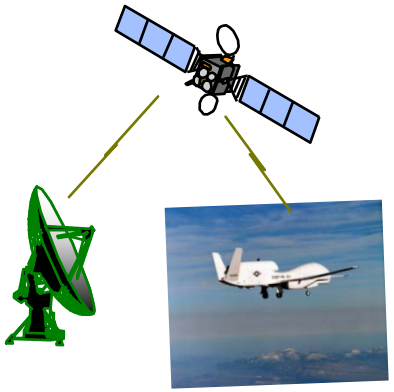
Reachback



Tactical
to
Tactical

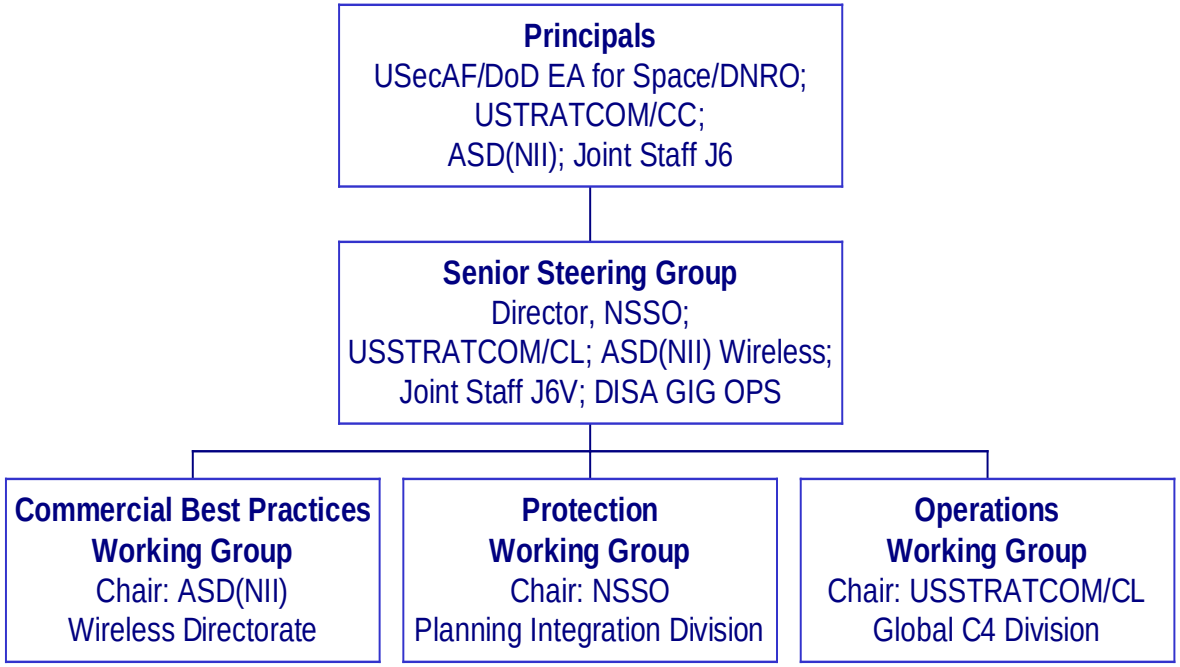


Broadcast



UAV

DoD Commercial SATCOM Study



(U) Working group participants include:

- (U) DoD stakeholders (OSD, Joint Staff, USSTRATCOM, Military Departments, DISA, NSA)
- (U//FOUO) Other federal stakeholders (including Homeland Security, State, FCC, DCI)
- (U) Communications satellite network operators, integrators and manufacturers

New Strategic Approach to SATCOM Acquisition

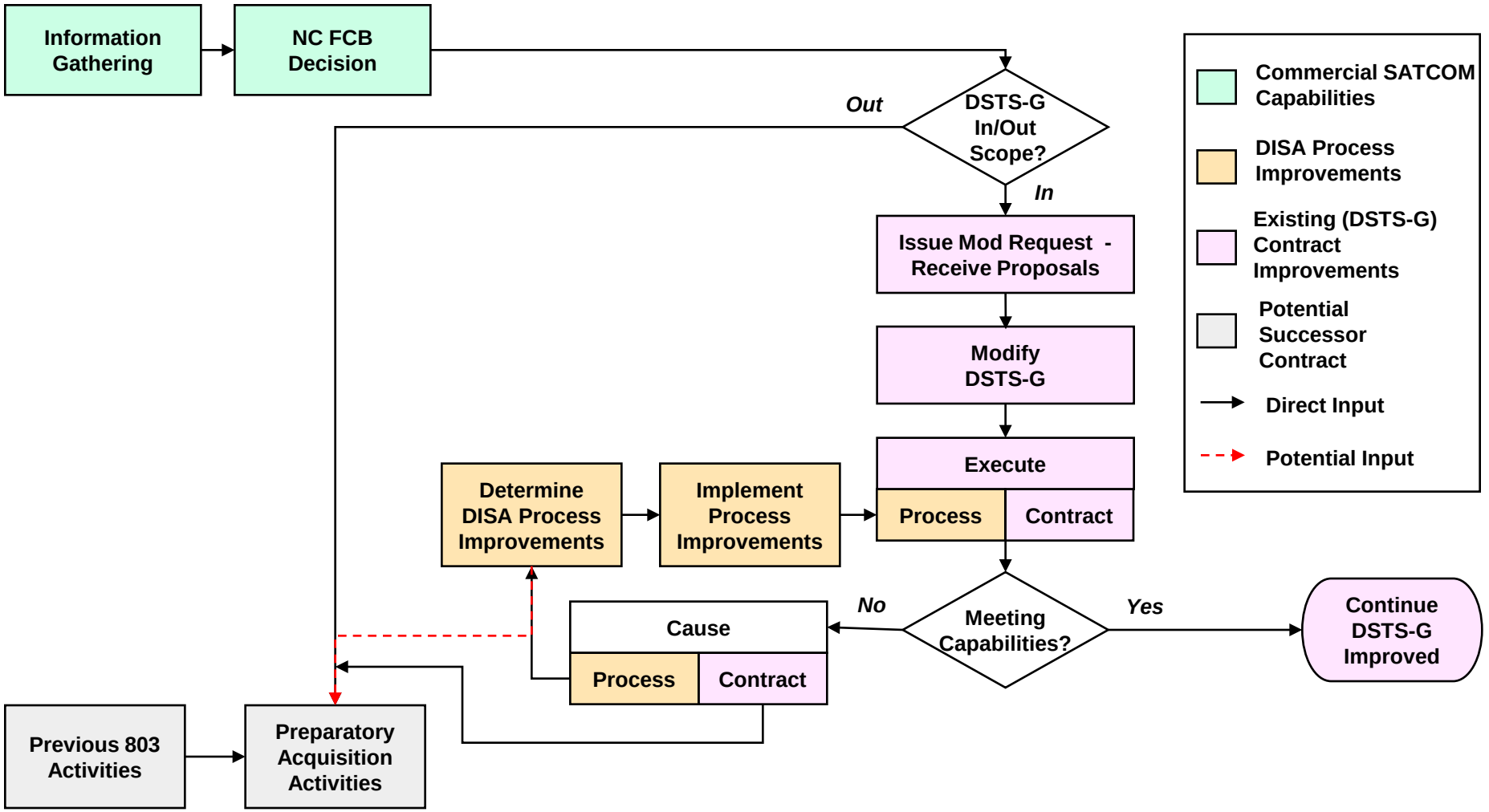
Phase 1

- **Improve operational effectiveness of existing contracts by incorporating changes to internal DISA processes to improve responsiveness; aggregate bandwidth to reduce cost**
- **Pursue warfighter requirements within the scope constraints of the current contracts**

Phase 2

- **Examine how best to craft successor a contract intended to:**
  - **Meet the full range of warfighter requirements as defined by the Net-Centric Functional Capabilities Board**
  - **Enable cost savings of bandwidth aggregation**
  - **Leverage lessons learned from modifications to existing contracts**

Commercial SATCOM Acquisition Strategy Revision



Protection Best Practice
Survey Team

- Col Thomas Shearer
  - Chief, Planning Integration Division, National Security Space Office
- Mr. Peter Marquez
  - Policy Analyst, Office of Space Policy, Office of the Undersecretary of Defense (Policy)
- Maj Robert Licciardi
  - Commercial SATCOM Operational Manager, USSTRATCOM J661
- Maj Brent McArthur
  - Lead, Protection Branch, NSSO Planning Integration
- Mr. Robert Abramson
  - Senior Engineer, The MITRE Corporation
- Mr. Richard Buenneke (Rapporteur)
  - Senior Policy Analyst, The Aerospace Corporation