Enterprise Architecture Special Interest Group (EA-SIG)
Enterprise Service Management Working Group (ESM)

Version 1.0 Draft
February 20, 2004

Prepared for the

Defense Information Systems Agency
NCES Program Office

By the

Open GIS Consortium, Inc. (OGC)
Enterprise Architecture Special Interest Group

Contributors

Matt Murray - Raytheon

Jeff Stollman - IBM

Shue-Jane Thompson – Northrop Grumman

Terry Plymell – Raytheon

Eli Hertz - SAIC

Chuck Heazel – Lockheed Martin

Disclaimer: This document represents the consensus view of the members of the EA-SIG Enterprise Service Management Working Group. The contents of this document do not necessarily represent the views or policies of the Department of Defense nor of the employers of working group members.

Enterprise Architecture Special Interest Group (EA SIG)

Enterprise Service Management (ESM)

White Paper

Change Log

Date	Author	Description	Version	Affected Pages
2/13/04	C. Heazel	Near-final draft	0.9	
2/17/04	Matt Murray	Updates throughout doc. Removed Use Case Section, Commercial Analog Section and ESM Contract Options Section. These sections have inputs but the inputs are incomplete and not mature. Will continue to work these sections and add them in the future.	0.9.1	All
2/19/04	Matt Murray	Added Recommendation Section and Appendix B – ITIL Framework	1.0	23-26
2/20/04	EA-SIG	Delivery of Version 1.0 to DISA	1.0	

Enterprise Architecture Special Interest Group (EA SIG)

Enterprise Service Management (ESM)

White Paper

Table of Contents

Enterprise Architecture Special Interest Group (EA SIG)

Enterprise Service Management (ESM)

White Paper

1 Introduction

Figure 1 depicts the broad scope of GIG Enterprise Services (GES). As the enterprise services component of the Global Information Grid, GES is the infrastructure on which DoD computer applications (e.g., C2, Combat Support, Medical) rely. GES in turn relies on the GIG transport services such as the Defense Information System Network (DISN) and tactical communications systems. DISN and tactical communications systems consist of transmission systems, distribution/switching systems, Video Teleconferencing (VTC) and packet and other support infrastructures.

While GES relies upon the GIG transport services for the exchange between the Core Enterprise Services (CESs) and the Community of Interest (CoI) capabilities, transport is not an inherent component of GES. There are nine CES:Application, User Assistance, Storage, Messaging, IA/Sceurity, Discovery, Mediation, Collaboration, and Enterprise Service Management (ESM) services. CES will be part of a common IT infrastructure that provides reliable, secure and efficient information delivery to decision makers and war-fighters.

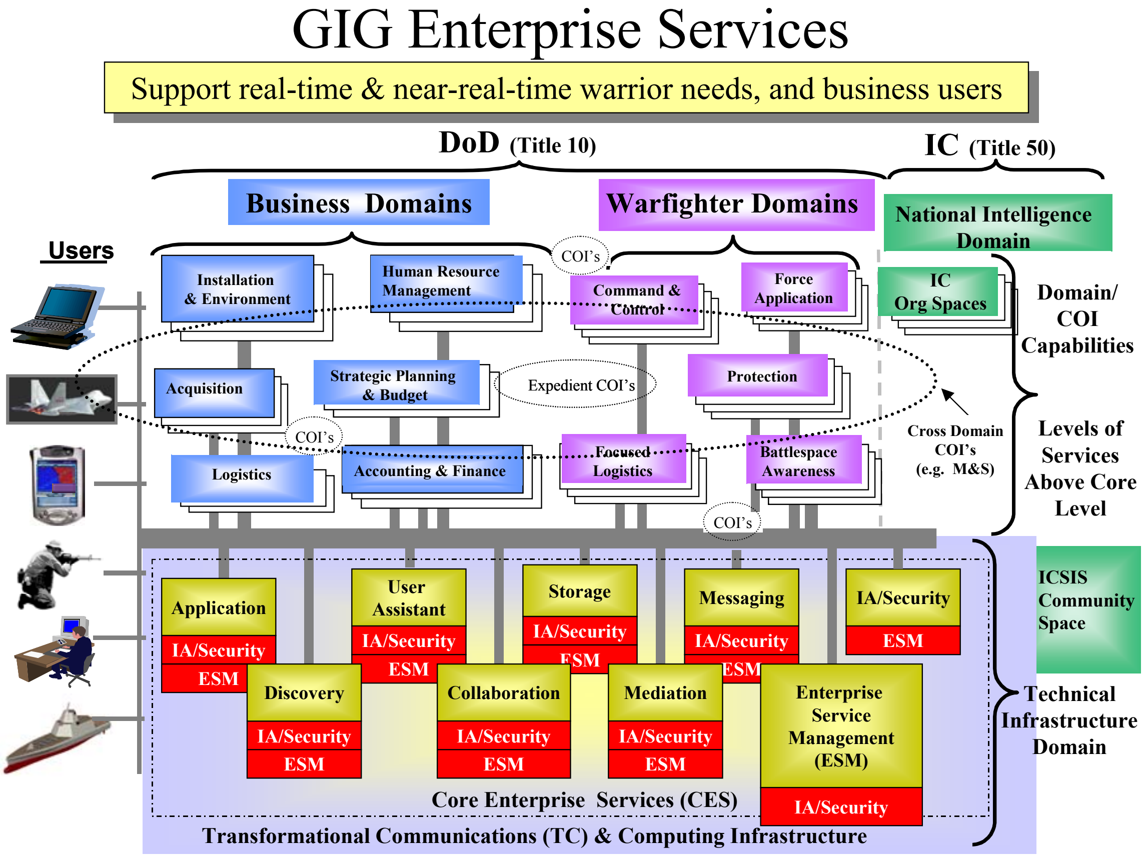
This document focuses on the goals, objectives, capabilities and recommendation for the ESM Core Enterprise Service. The charter for this team was to address three fundamental questions:

What it Enterprise Service Management?

What can we buy or build today?

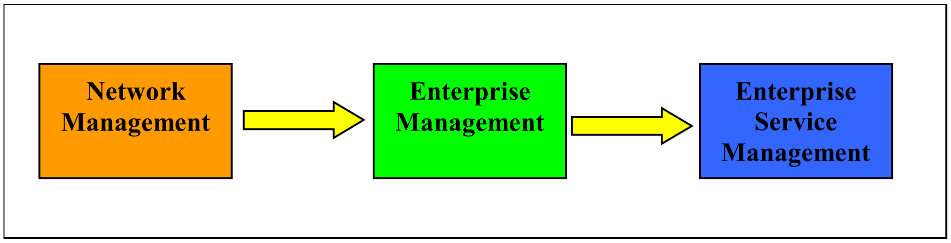
How should we invest for the future?

This paper responds to those questions by defining and describing ESM, discussing what is being done today, and what the group sees for the future of ESM?



2 Scope

Mission operations today are heavily dependent to the enterprise IT capabilities. Traditional network management that focuses merely on status monitoring and fault recovery of the transport layer components is no longer sufficient. Successful mission performance requires end to end process results which meet the standards set for that process. Therefore, the trend of ever increasing importance of IT capabilities has triggered rapid evolution of IT infostructure management. Traditional node based or component based monitoring and reporting is no longer sufficient. Many new technologies evolved to mitigate the capability gaps, correlation and analysis engine, root cause analysis capability, event aggregation and suppression, web-based user interfaces, service level management, etc…



Enterprise Service Management Evolution Path

Network management – Focuses on transport layer monitoring and fault recovery. A reactive management style supporting network engineers and administrators by detecting infrastructure faults (mainly in network) and alert them for the fault detected.

Enterprise Management – Focuses on Fault, Configuration, Accounting, Performance, and Security (FCAPS) management areas. It expands the management scope from just network node up and down status to include network, systems, storage, and applications health status.

Enterprise Service Management (ESM)- Focus on over all service performance and performance objectives that are agreed as stated in a Service Level Agreement (SLA) or other type of understanding or agreement document such as a Memorandum of Understanding (MOU), a Memorandum of Agreement (MOA), or an Operational Level of Agreement (OLA). ESM focuses on managing the end users' experience. Service planning is driven by the users requirements and success is based on whether or not the required service performance is met.

Traditional network operation center (NOC) or today's Network operation and security center (NOSC) focuses on infrastructure operation status, mainly on network, system and application availability, and fault recovery. Often these centers are not seamlessly integrated with IT service planning, provisioning, or customer services etc. Without end to end service management capability, overall service performance status is an unknown. Thus, IT service quality assurance is often reactive and only managed by incidents; we must now become proactive and be concerned with the end to end performance.

3 ESM Description

Enterprise Service Management (ESM) "focuses on selecting, sizing, and loading those applications that operate the GIG infrastructure or are used to administer the GIG infrastructure (e.g., Operating Systems, System Utilities, Data Management Systems, Auditing Software, and System Management and Reporting Applications, Monitoring Software). NetOps personnel perform this activity. It takes hardware configurations, GIG architecture information, and Standard Net-Centric Operating Procedures, and supplies system applications that run and manage the GIG." – *NCOW*

"[ESM] is the set of services provides end-to-end GIG performance monitoring, configuration management and problem detection/resolution, as well as enterprise IT resource accounting and addressing, for example, for users, systems and devices. Additionally, general help desk and emergency support to users is encompassed by this service area, similar to 911 and 411. – D. Meyerriecks, *Net-Centric Enterprise Services*

Enterprise Services Management (ESM) provides a suite of processes, procedures and services – capabilities that ensure that GIG Enterprise Services are up and operating within tolerances specified in Service Level Agreements (SLAs) to achieve the Department's objectives. As such, ESM requires a wide range of capabilities including:

- Establishing Service Level Agreement (SLA) and Quality of Service (QoS) objectives
- Enterprise level monitoring of global net configuration
- Enterprise activity auditing
- Infrastructure and service management
- Performance quality management
- Survivability and Fault Tolerance fail-over
- Maintenance of supporting policies and procedures

In a net-centric environment, the operational management of the underlying infrastructure becomes a mission-essential task. In many cases mission critical services are increasingly dependent on distributed net capabilities that must be managed end-to-end. To support mission critical services, the underlying infrastructure should be planned, built, sized, implemented, operated and managed to meet target, end-state GIG operational requirements.

Further, ESM solutions for non-deployed and deployed environments must be:

- capable of supporting 7x24x365 operations
- at least as reliable as the systems they support
- meet current and emerging security requirements
- be interoperable across traditional organizational enclave boundaries
- be easy to use and maintain with effective service desk support.
- Be scalable and modular to allow for the future addition of capabilities or to replace underlining technologies or products.

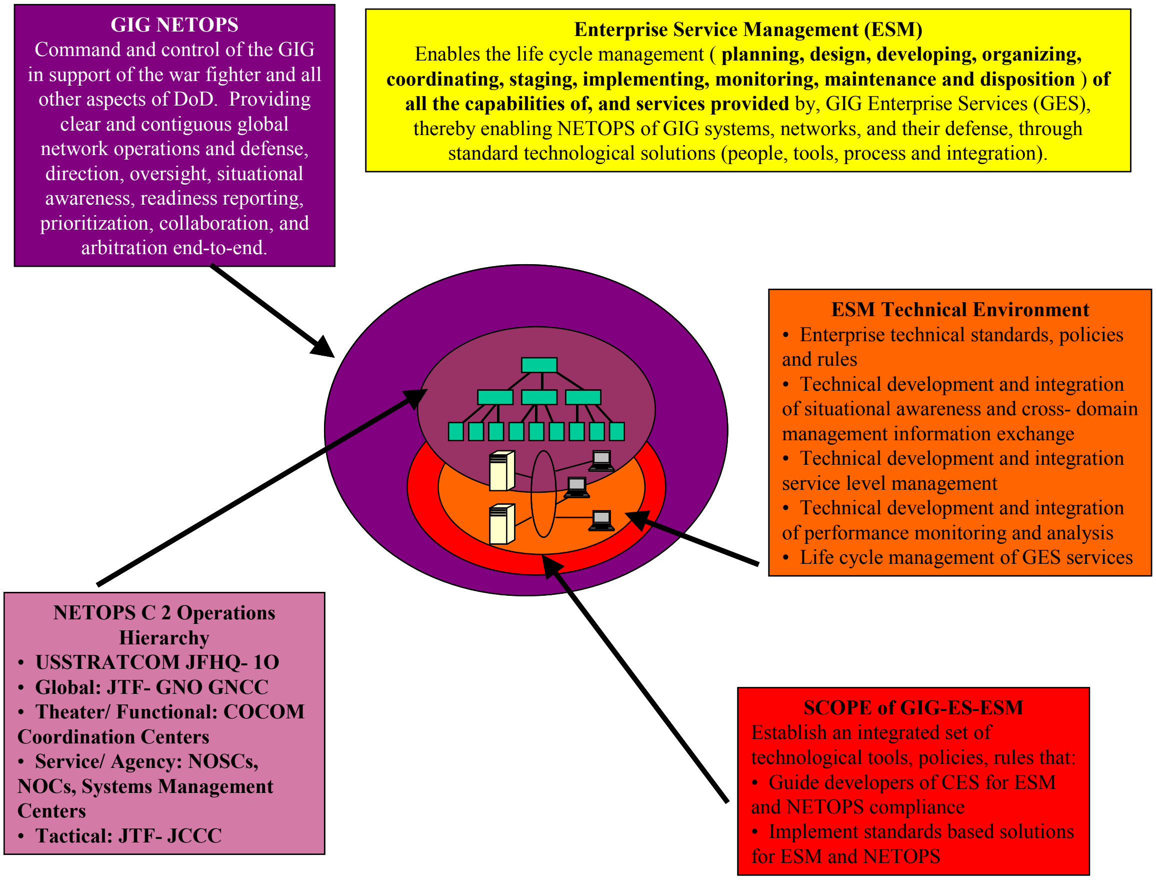
Enterprise Service Management enables the life cycle management of all the capabilities of, and services provided by the GIG Enterprise Services (GES), thereby enabling NETOPS of GIG systems, networks, and their defense, through standard technological solutions (people, tools, process and integration). Activities covered by ESM include:

- planning,
- design,
- development,
- organization,

- coordination,
- staging,
- implementation,
- monitoring,
- maintenance and
- disposition.

Command and control of the GIG in support of the war fighter and all other aspects of DoD providing clear and contiguous global network operations and defense, direction, oversight, situational awareness, readiness reporting, prioritization, collaboration, and arbitration end-to-end.

Figure 2 provides an overview of the relationship between Enterprise System Management (ESM) and Network Operations (NETOPS). The combination of the two results in the guaranteed and secure delivery of information to the war-fighter.



GIG NETOPS
Command and control of the GIG in support of the war fighter and all other aspects of DoD. Providing clear and contiguous global network operations and defense, direction, oversight, situational awareness, readiness reporting, prioritization, collaboration, and arbitration end-to-end.

Enterprise Service Management (ESM)
Enables the life cycle management (**planning, design, developing, organizing, coordinating, staging, implementing, monitoring, maintenance and disposition**) **of all the capabilities of, and services provided** by, GIG Enterprise Services (GES), thereby enabling NETOPS of GIG systems, networks, and their defense, through standard technological solutions (people, tools, process and integration).

ESM Technical Environment
- Enterprise technical standards, policies and rules
- Technical development and integration of situational awareness and cross- domain management information exchange
- Technical development and integration service level management
- Technical development and integration of performance monitoring and analysis
- Life cycle management of GES services

NETOPS C 2 Operations Hierarchy
- **USSTRATCOM JFHQ- 1O**
- **Global: JTF- GNO GNCC**
- **Theater/ Functional: COCOM Coordination Centers**
- **Service/ Agency: NOSCs, NOCs, Systems Management Centers**
- **Tactical: JTF- JCCC**

SCOPE of GIG-ES-ESM
Establish an integrated set of technological tools, policies, rules that:
- Guide developers of CES for ESM and NETOPS compliance
- Implement standards based solutions for ESM and NETOPS

Figure 2 – NETOPS + ESM = Assured network availability, assured information delivery and assured information protection – end-to-end

3.1 ESM Capabilities

A summary of ESM capabilities, description of service and industry examples of the ESM services (as they would apply to GIG operational support) is provided in Table 1.

NCES Enterprise Service Registry	
Description: ESM shall operate and maintain the "catalog" of GIG Enterprise Service offerings to include developing, deploying, operating, and maintaining the processes and technical solutions necessary for IT service offerings to be registered and advertised, e.g. a UDDI registry for GIG Enterprise Services based on Web-service implementations along with other technical solutions as may be required to register and advertise non-Web-service based service offerings.	**Functions:** • Efficient registration of services to be managed (NCES and domain specific services)
Configuration Management	
Description: ESM shall provide an automated and manual Configuration Management (CM) capability for NCES configuration items including security, for example hardware, software, and system/service documentation as well as for non-NCES hosted, provided, or supported customer configuration items operating in, resident on, or relevant to NCES operations and the NCES operational environment. NCES CM data shall include both non-operational and operational characteristics, e.g. serial numbers as well as router port assignments. NCES CM data shall be made available electronically in a standard format to other NCES and non-NCES services as required.	**Functions:** • Problem/Change Management • Hardware/Software Asset Management • Application Management • Security Management
End-to-End Performance Monitoring and Analysis	
Description: ESM shall provide the capability to continuously monitor and analyze the performance of individual service elements, components, connections and/or the end-to-end performance of NCES services. Key elements of performance management are:	**Functions:** • SNMP Core Framework • Network/Host/Device Management • Fault Detection/Fault Isolation • IS Analysis and Reporting • Service Level Management • Performance Baseline & Optimization • Performance Trending • Capacity Planning • Threshold Monitoring
NCES Service Life-Cycle Management	

Description: ESM shall provide a service life-cycle management process that ensures the integrated and synchronized planning, design, development, provisioning, deployment, operation and maintenance, management, and retirement of NCES services.	**Functions:** • Life Cycle management of assets and services • Efficient and automated 'hand-off' of new services to on-line ESM/NETOPS • Provides a defined base line and environmental frame work for planning design and development.
NCES Infrastructure Management	
Description: ESM shall provide an integrated operational infrastructure management capability for NCES LANs and supporting communications equipment, e.g. CSU/DSUs, that provide connectivity to WANs and other transport systems as well as for non-IT systems and services as may be required. Infrastructure management capabilities shall include robust and secure fault, configuration, accounting, performance, and IA/security management (FCAPS) of NCES infrastructure components as well as capacity, availability, and scheduling management.	**Functions:** • SNMP Core Framework • Network Management • Host Management • Application Management • Facility Management • Internet Services Management • Database Management
Integrated Service Management	
Description: ESM shall provide an integrated operational enterprise service management capabilities to include robust and secure fault, configuration, accounting, performance, and IA/security management (FCAPS) of all NCES services (and of their sub-services, elements, and components) as well as capacity, availability, scheduling, and storage management. In addition to commonly required management capabilities, the NCES ESM service shall also develop capabilities that address the specific or unique requirements of each NCES service, e.g. managing a messaging service requires a somewhat different set of functional capabilities and technical solutions than what may be required to manage a discovery service and vice versa.	**Functions:** • Service Level Management • User Interface/Centralized Status Console • I/S Analysis and Reporting Services
Cross-Domain Management Information Exchange	
Description: ESM shall be fully able to seamlessly and securely exchange required management information between Combatant Command, Service, Agency, Allied, and Coalition operational IT management domains as governed by NCES and other applicable security policies. This attribute does not include the automated exchange of management information between different security	**Functions:** • Establish and track SLA between NCES and Domains • Interface Control Definitions for the efficient exchange of management information

levels or boundaries, e.g. between NIPRNet and SIPRNet or across a US-to-Coalition network boundary.	
NCES Service Level Management	
Description: ESM shall provide the capability to create, measure, monitor, manage, and enforce negotiated Operational and/or Service Level Agreements (OLA/SLAs) governing the end-to-end delivery of each GIG Enterprise Service and its sub-services, elements, and components. OLA/SLAs may be negotiated and created between one or more service providers as well as between a service provider and its customers and may be implemented across one or more management domain.	**Functions:** • Service Level Management • User Interface/Centralized Console
NCES Quality of Service (QoS) Management	
Description: ESM shall provide the capability to measure, monitor, manage, and enforce Quality of Service (QoS) mechanisms that are developed and deployed to ensure that NCES service related traffic is processed and delivered based assigned priorities. While ESM is not directly responsible for the development and deployment of NCES QoS capabilities, ESM shall coordinate the development and approve the deployment of all NCES QoS capabilities to ensure that they are compatible and interoperable. ESM shall also coordinate NCES QoS capability development with GIG network and transport service providers, e.g. GIG-BE, TCI, JTRS.	**Functions:** • Service Level Management • Component / Element Management • Fault Management
NCES Operational Process Management	
Description: NCES ESM shall develop and utilize an operational process model that supports the rapid identification, tracking, resolution, and documentation of NCES-related incidents, reported problems, and service requests to ensure the quick restoration of NCES services with the minimum impact to the user. NCES operational processes shall be based on industry standards, e.g. Information Technology Infrastructure Library (ITIL) and Telemanagement Forum (TMF), and accepted best practices and lessons learned from government and commercial organizations responsible for IT operational management.	**Functions:** • ESM tool and process support and integration of NETOPS
NCES NETOPS Situational Awareness	
Description: NCES shall provide managers at all levels with comprehensive and relevant NETOPS situational awareness that will enable them to determine the end-to-end operational status and	**Functions:** • Integration with NETOPS

associated mission or business impacts of any NCES service (or combination of services) in near real time. This will require close coordination and the exchange of relevant management information at multiple levels with the organizations, facilities, and systems responsible for the operational management of GIG network and transport services.	
Information Assurance/Security	
Description: ESM capabilities shall meet applicable DoD and/or DCI Information Assurance requirements. IA/Security CES should be integrated into the ESM CES to ensure the protection and operations of the GIG.	**Functions:** • Integration with Security operation center, tools and process to provide a complete picture of the operations and seciuirty of the GIG • Correlation of security events with Enterprise events (network, servers, application, data…..) • Security of the ESM 'application and data'
Enterprise Service Desk	
Description: ESM shall provide a service desk capability to support NCES user and customer incident and service request reporting, prioritization, tracking, management, and resolution.	**Functions:** • Customer interface – help desk and service desk functions • User sastisfaction
Enterprise Software Distribution	
Description: The ESM Software Distribution capability shall verify that all software or documentation has been obtained from authorized sources before making it available for use.	**Functions:** • Software distribution, remote monitoring, analysis, version control • Document management
NCES User Provisioning and Profile Management	
Description: ESM shall provide automated and manual user account and dynamic profile management capabilities that will enable the management and administration of enterprise users and their corresponding profiles to include passwords, preferences, and establishing access to enterprise services. This service offering will be closely coordinated with supporting IA/Security and User Assistance services.	**Functions:** • User Management • Directory services • Password/access management
ESM Support for Disconnected Operations	
Description: ESM shall be able to effectively manage NCES services and users when they become isolated or disconnected from a service through a fault in the service, in a supporting	**Functions:** • Dial up management capabilities

service, or through a fault in the underlying transport or communications networks. ESM shall be capable of identifying when a user has become isolated and alert other NCES services to which the user is subscribed to ensure that any service is delivered via alternative means, queued for later delivery, etc. ESM shall also be capable of notifying NCES services when disconnected users are restored to service.	• Push software via Web services • On-board diagnostic tools, self help tools • Automated installation of management data via CD or Web • Process to support users via phone, PDA or walk in
Remote Management	
Description: ESM shall provide the capability to perform remote service element and component configuration/reconfiguration of existing non-NCES systems, services, and components that have management capabilities.	**Functions:** • Agent technology that provides dial up or direct connect access to geographically disperse IT assets • Ability to manage across low band width • Software distribution • Analysis and problem resolution • Re-configuration
Survivability	
Description: ESM capabilities shall be protected against all potential threats commensurate with the identified NCES threat environment and shall ensure continuity of NCES service operations in a manner that assures that services meet Operational and Service Level Agreements (OLAs/SLAs). Threats include but are not limited to physical threats such as fire, water damage, power outage, natural events, and information operation or electronic threats such as cyberattack or Electromagnetic Pulse (EMP). Where applicable the elements in the OLAs/SLAs shall be implemented in the local digital policy and in some cases the organizational level digital policies.	**Functions:** • COOP capabilities • Redundancy • Backup/Recovery

Table 1 - ESM Capabilities

3.1.1 ESM Interface with Core Enterprise Services (CES)

NCES Core Enterprise Services (CES) identify nine critical IT capabilities that are required for efficient, guaranteed and secured end-to-end Net-Centric capabilities. Of these nine capabilities, Enterprise Services Management and Information Assurance/Security have the objective to ensure the operation and security integrity of Net-Centric services.

A key underlying tenet of CES Enterprise Services Management is that all CES and Community of Interest (CoI) services must be “manageable” in all deployed operational environments. This means that they must be equipped or instrumented with the appropriate set of built-in ESM capabilities and that they must support agreed upon operational policies, processes and procedures. For NCES Increment I this means that every CES and CoI service must be able to securely monitor, detect changes in, and publish:

- The activity of critical processes and resource utilization and accurately and securely report anomalous behavior that breaches agreed upon thresholds
- Their operational configuration and accurately and securely report any changes in configuration or operational status
- Their overall operational performance and accurately and securely report any failure to meet agreed upon service level agreements

Their security status and to accurately and securely report on any changes in security status to include any anomalous security behavior that could be indicative of a cyber-attack directed against the service

In addition, all deployed services must:

- Meet minimum DoD IA requirements as outlined in DoDD 8500.1 Information Assurance and DoDI 8500.2 Information Assurance Implementation
- Provide adequate and timely service desk support and
- Support CES EMS trouble identification, reporting, escalation, resolution and notification processes and procedures

This means that ESM will be an integral set of capabilities that must be built-into every CES and COI service whenever possible, as well as being a stand-alone service or functional capability that will be used to proactively management critical NCES components. COTS and 3rd party software components not engineered to interoperate with ESM will need to be brought into the fold via service mediators or other bridging technologies (such as SNMP).

To accomplish this, the ESM will develop guidelines that other CES and COI services must follow in implementing their management capabilities as well as compliance criteria that will be used to ensure that management capabilities are correctly implemented.

3.2 Service Level Management (SLM) Overview

Service-level management (SLM) is critical in order to define, achieve, and maintain required levels of NCES services in support of the warfighter and all users. SLM provides a way to maintain accountability, whereby availability and reliability of applications, servers, and networks that affect a service can be easily tracked and maintained according to agreed upon guidelines. Resulting metrics contribute to defining and meeting service-level agreements (SLAs). It is imperative that sound processes linked with people skill-mix and organizational structure exist to successfully realize SLM objectives. According to Sturm, Morris and Jander in *Foundations of Service Level Management*, a good service level agreement:

- “Provides permanence
- Provides clarity
- Serves as a communications vehicle
- Guards against 'expectations creep'
- Sets mutual standards for service
- Defines how a level of service will be measured"

There are three basic types of SLAs, and they are:

- ***In-House SLA*** - This is an agreement negotiated between the service provider, such as an IT department, and an in-house user department. Don't assume that because the SLA is negotiated between two departments in the same company, that the agreement is without teeth. Because the nature of some companies' business requires significant levels of availability, they have in-house SLAs in place with their IT departments that require 100% availability. And this level of service can actually be used as a selling point to external customers.
- ***External SLAs*** **-** External SLAs are agreements that any company that's purchasing services such as IT from an external provider like an ASP or MSP can't be without. If a company gets less-than-acceptable service from its ASP, for example, and does not have an SLA in place, that company may not have many options to either force the ASP to address the problem or terminate their contract without penalties. Conversely, if a company does negotiate an SLA with a service provider, the agreement should be reviewed by an attorney before signing, since it is a legally binding contract.
- ***Internal SLAs*** - These types of SLAs are usually informal agreements within a department for achieving certain performance goals, and for measuring progress in achieving those goals. They may not even be written as separate documents, but may be part of other plans such as individual achievement goals for the purpose of receiving bonuses.

Creating an SLA must begin with serious commitments from top-level managers from both the service-provider and the user groups to negotiate a fair and equitable agreement. The agreement should be negotiated on as level a playing field as possible: the group actually given the task of negotiating the agreement should comprise equal numbers of individuals from both stakeholder groups, and the leaders representing each stakeholder should have nearly the same rank within the organizational hierarchy. A good rule of thumb to follow regarding the size of a negotiating group is, for a medium-to-large company, there should be four to 10 individuals.

Each member of the negotiating team should have some unique expertise to bring to the process, like in-depth business knowledge about how the service affects the user department's productivity or bottom line or knowledge about the technology that the service provider needs to provide the requested service level. At the onset of negotiations, the group leaders should write a charter for the group defining aspects like group responsibilities, membership, functions and so on.

To expedite the process, all constituents should know certain specifics about the agreement ahead of time, if possible provide a “strawman” or proposed SLAs. The negotiators must understand the cost and the variables for the proposed level of service and the benefits of the service level being requested. Additoinally , the group should have information available about the current service levels and how the services are measured.

Beyond defining who are the parties in the SLA (i.e., the service provider and the customer), a number of components make up an SLA, including the following:

- ***Term*** - defines the period of time that the SLA will cover. This is usually no more than two years, since technology will advance too fast for a longer-term agreement to be meaningful. An industry best practice is to review the SLA annually to insure the proper metrics are being measured and that the focus of the metrics are consistent with the prorities of the enterprise.
- ***Scope*** - defines the services covered in the agreement. This might include what specific business process will be covered, which users of this process will be covered, at what times during the day/week will the service-level requirements be effective, and so on. This section does not cover the service levels to be provided.
- ***Limitations*** - defines what must happen in order for the requested service levels to be provided. This includes items like what volume of transactions the service provider might be required to

handle, the cost of hiring the staff necessary to provide the levels of service, and so on. The bottom line is, service providers have to believe they can really provide the required levels of service before they agree on them. To keep the SLA realistic, they must build into the agreement limitations that take into consideration future variables like growth in demand, opening or closing user facilities and integrating disparate computing systems into the current one.

- ***Service-level objectives*** - are the levels of service that both the users and the service providers agree on, and usually includes availability, performance and accuracy. Each aspect of the service level, such as availability, will have a target level to achieve. (But the agreement *might* include two measures for each aspect: a minimum-acceptable level of service to achieve, and a stretch level of service that the provider should aim to achieve and can be rewarded for achieving.) Availability can be measured in units of time (e.g., hours or days) or in percentages. Performance can be measured by volume of work accomplished (e.g., transactions) or speed. Accuracy can be measured in terms of whether or not the service is doing what it should be doing. Note: In an SLA, there is no *right number* of service-level objectives - aim for between five and ten.
- ***Service-level indicators*** - the means by which these levels can be measured. The best way to measure service levels is from the user's perspective - how much time were the services that users need to do their jobs or to do business available and how responsive were the services? However these user perceptions are measured, the SLA will need to document each service-level indicator used to measure the objectives, and to specify the data source for each.
- ***Nonperformance*** - spells out what happens if the service provider does not meet the objectives in the SLA. If the agreement is with an external service provider, the option of terminating the contract in light of unacceptable service levels should be built in. Nonperformance penalties can range from a rebate of a percentage of what an external service provider is charging annually in maintenance fees to a mandatory meeting between the service provider's and the user's top executives to discuss the service lapse. But whether the SLA is in-house or external, penalties can be important for the SLA to have real meaning for everyone concerned.
- ***Optional services*** - provides for any services that are not normally required by the user, but might be required as an exception. An example of this would be extra hours of IT service for an e-business during the busy Christmas shopping season.
- ***Exclusions*** - specifies what is not covered in the SLA. Reporting - is a key component of SLM. These provide the means to determine whether or not the service provider is living up to its commitments in the SLA. So, the reports must be relevant to these objectives, must reflect the means of measuring the objectives stated in the SLA, and they must be communicated so that the audience they are intended for can understand them. When discussing reporting requirements, an SLA should include information such as the name of each required report, the frequency that each report will be generated, and the content of each report.
- ***Administration*** - describes the processes created in the SLA to meet and measure its objectives and defines organizational responsibility for overseeing each of those processes.
- ***Reviews*** - establishes regularly scheduled reviews between the user and service-provider constituents of an SLA.
- ***Revisions*** - provides for any revisions necessary to keep the SLA extant for all parties.
- ***Approvals*** - Signatures on the dotted line: the SLA is signed, sealed and delivered.

3.3 Quality of Service (QoS) Overview

Quality of Service has two meanings in the ESM space. First, it generically refers to the fact that different tiers of service may be offered for the same functionality. Second, it is used to refer to the ability of a single IT resource (e.g., the network or a server) to provide distinctly different service levels. These are discussed separately below.

Quality of Service as a service tier

In the enterprise IT space, not all services need to adhere to the same service levels. The availability and responsiveness requirements of a service component within the "sensor-to-shooter" process a similar component used to process an overnight business batch job. To provide a single service level for enterprise availability and enterprise responsiveness would either jeopardize mission effectiveness in the "sensor-to-shooter" area or drive inordinate cost across the enterprise to support higher than needed service levels for back-office functions. It is, therefore, valuable to segregate the various IT services offered into tiers or service.

Currently, to devise separate tiers for each and every service would require too much manpower to establish the specific service levels for each service. Accordingly, common practice is to offer three levels of service (often referred to as Gold, Silver, and Bronze) and cluster services into one of these as a reasonable trade-off between service levels and cost. There are no fixed service levels associated with these three categories. Neither is there any magic about the number three. Three levels provides flexibility without making the process unmanageable.

Quality of Service as a way to segregate the services offered by a single resource

Quality of Service (especially when used in the abbreviated form, "QoS") is commonly used to refer to the ability to divide the service supplied by a single resource to give yield different service levels for different users of the same service. For example, the entire concept of "grid computing" is predicated on server management software that can provide resources to a primary application on an as-needed basis, and scavenge remain cycles to support an additional application that will take whatever it can get. The guaranteed level of service afforded the servers primary application is called its QoS.

Another more pressing example is network bandwidth where QoS is cited as the primary barrier to widespread use of Voice over IP (VoIP). Currently, Internet Protocol as implemented in todays routers does not offer QoS. Network packets (whether data, voice, or video) are dynamically routed on a best-efforts basis. This "best-efforts" process results in the data getting from sender to receiver, even when parts of the network fail during the transmission. During a failure, packets are just rerouted to other parts of the network that are available. As a result, different packets in a transmission may take different routes and arrive at the destination at different times. This is generally adequate for data traffic because data will be recombined at the destination, regardless of what order it arrived in. However, for audio traffic (e.g., VoIP) the transmission is "live" and the out-of-order packets will "play" in the order in which they are received, resulting in garbled audio. The problem can be worse for video. For video traffic, the transmission can be lost from the point at which the network had to reconfigure the routing of the transmission. And for encrypted traffic, the entire message can be lost. What is needed is the ability to guarantee not only the successful transmission of a message from Point A to Point B, but also a guarantee that the packets will arrive in order: maintaining the integrity of audio, video, and encrypted messages. This guarantee is called QoS.

Solutions exist to solve this problem, but one has not yet become the international standard. These solutions support multiple levels of QoS so that traffic can be prioritized. This prioritization not only allows message integrity to be guaranteed, but it also allows messages of high-priority to "bump" (or reduce available bandwidth for) messages of low priority in order to optimize the available bandwidth. For example, tactical direction from headquarters to a field unit could preempt the transmission of a movie being sent across the network to entertain the troops.

4 Technology Analysis

4.1 ESM Standards

Enterprise Service Management has evolved a long way from the early days of Network Management, System Management, Enterprise Management to today's service objectives of Enterprise Service Management. The standards have also evolved from early versions of Open Systems Interconnect Simple

Network Management Protocol (SNMP) and the very popular FCAPS (Fault, Configuration, Accounting, Performance and Security) framework to the new and evolving service based IT Information Library (ITIL) developed by the Office of Government Commerce (OGC) reporting to the Chief Secretary to the Treasury, British Government. Figure 5.1 provides an overview of the current set of standards that can be utilized in developing NCES's ESM capability.

Standard & Supporting Organization	Overview (including objective)	Maturity
IETF Simple Network Management Protocol (SNMP)		
OSI Common Management Information Protocol (CMIP)		
OSI's FCAPS Framework		
Distributed Management Task Force (DMTF) – Web-Based Enterprise Management (WBEM) **[formally Desktop Management TF]**		
DMTF's Desktop Management Interface (DMI)		
DMTF's Common Information Model (CIM)		
OMG's CORBA		
WWW Consortium - SOAP		
Organization for the Advancement of Structured Information Standards (OASIS) - Web Application Security (WAS)	To produce a classification scheme for Web security vulnerabilities, a model to provide guidance for initial threat, impact and risk ratings, and an XML schema to describe Web security conditions for use with assessment and protection tools.	New – started May 2003
Web Services Distributed Management (WSDM)	To define Web services management; to use Web services architecture and technology to manage distributed resources, and to develop the model of a Web service as a manageable resource.	New – started February 2003, with V1.0 due February 2004
Storage Network Industry Association (SNIA), Storage Manage Initiative Specification (SMI-S)	Provide storage customers a way to manage multiple storage appliances from different vendors. Before the proposed specification, enterprise storage managers would have had to manage each storage appliance with vendor-specific tools and work to integrate the disparate information manually	New – Expected to announce Version 1.0 of SMI-S July 2003
The Open Group's Enterprise Management Forum – Various Standards and technical guides on Systems Management	Industry lead consortium establishing standards and technical integration for systems management	Mature, been in existence since 1995

OGC's IT Infrastructure Library (ITIL)	ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally. It is supported by a comprehensive qualification scheme, accredited training organisations, and implementation and assessment tools. The best-practice processes promoted in ITIL both support and are supported by the British Standards Institution's Standard for IT Service Management (BS15000).	

Figure 5.2 – ESM Standards Overview

Web Services represent a new paradigm of computing, based on standards for various facets of software development and usage. Essentially they are business functions or services invoked, described, published, and interacted with using XML based standards. The attractiveness of the web Services concept lies in the universal adoption of standards by all vendors alike. This adoption promises to allow seamless interoperability among the different heterogeneous implementations. Standards are essential to Web Services and Enterprise Service management (ESM) and are the drivers for their use in integration.

The question of what technologies are available today for managing Web services may be like putting the cart before the horse, as few organizations have advanced beyond the pilot stage in their Web service projects. Consequently, most early adopters have relatively few Web services to manage. That message about what Web services and how to use them grew loud and clear from last years conferences.

Compounding the uncertainty in Enterprise Service Management is the lack of a firm standards roadmap beyond the SOAP, WSDL and UDDI building blocks, or the existence of best practices to deploy Web services. Today, managing Web services is still the domain of service providers or start-up vendors. Aside from service provider approaches, most of the current ideas rely on agents, probes, brokers or proxies to monitor and, in some cases, adjust parameters ranging from authorizations to component dependencies and code validation.

In general, the argument for brokers is that the technology is well established in the J2EE and Microsoft .NET worlds. Consequently, if a firm knows IBM WebSphere or Microsoft Windows Servers, they should be capable of getting up to speed with Web services brokering tools pretty readily. A drawback to brokers is that they introduce potential bottlenecks and single points of failure to environments likely to have numerous tiers.

For instance, Actional Corp., Mountain View, Calif., uses proxies that play traffic cop to incoming SOAP messages. On the horizon, it also plans to add agents that would reside on app servers and provide higher-level views of an entire service network. Iona Technologies, Waltham, Mass., is focusing more on the development and deployment, rather than the management, of Web services.

Talking Blocks Inc. provides security features aimed at managing authentication and access monitoring capabilities that log messages and provide the raw data for tracking utilization and generating alerts, as well as performance management features such as load balancing and routing. Infravio Inc., promotes its life-cycle management capabilities by providing several different views, including business objects, that provide a schema-based logical view; a business service that provides a mechanical view of how the message is transformed, transported and orchestrated; and an application model that focuses on brokering services.

Providers such as AmberPoint Inc., Flamenco Networks, Mindreef Inc. and Blue Titan Software Inc. provide distributed, probe-like approaches that "sniff" SOAP messages over the wire, but for different purposes. Mindreef Inc., focuses more on developers by providing debugging abilities through viewers that display the content of SOAP messages or WSDL files as either raw XML or pseudocode -- stripping out the ubiquitous angle brackets and showing the remaining XML as plain English. To help with the debugging process, Mindreef's tools trace SOAP messages to verify whether they execute properly.

AmberPoint takes an operations-oriented view. For instance, AmberPoint Inc. tracks performance and transactions by type or business process, such as the number of orders or shipment requests processed, and response times for those requests. Proxies intercept incoming requests and accept and redirect them, while plug-ins run inside the application server.

Today, products such as Tivoli, Patrol, Unicenter and OpenView have agent technologies that can actively manage infrastructure elements and activate alerts and consoles that provide the big picture on services levels at the node level. Measuring traffic levels, response times, and the stops and starts of specific operations is already second nature for most of the brand-name framework tools. Currently, these tools do not probe inside a SOAP message or inspect its headers, but they can record end-to-end performance data about when messages are sent or received, and how long it takes to process them.

Conceivably, another obvious point for managing Web services might be at the app server in the Java world, or the OS for .NET. For instance, many middleware platform providers have consoles for configuring and monitoring code execution, clustering, transaction pooling, load balancing and failover. Yet players such as Microsoft have been conspicuously silent, while others have largely deferred to third parties.

Having set the stage for a need for Web Services Management standards, Web services manageability is defined as a set of capabilities for discovering the existence, availability, health, performance, and usage, as well as the control and configuration of a Web service within the Web services architecture. This implies that Web services can be managed using Web services technologies.

Figure 5.2 shows the generic Web Services Stack as proposed by the W3C Web Services architecture group. Though the Web Services stack provides standards for service description, messaging, registry and security, a standard for Web Services management is yet to be addressed.

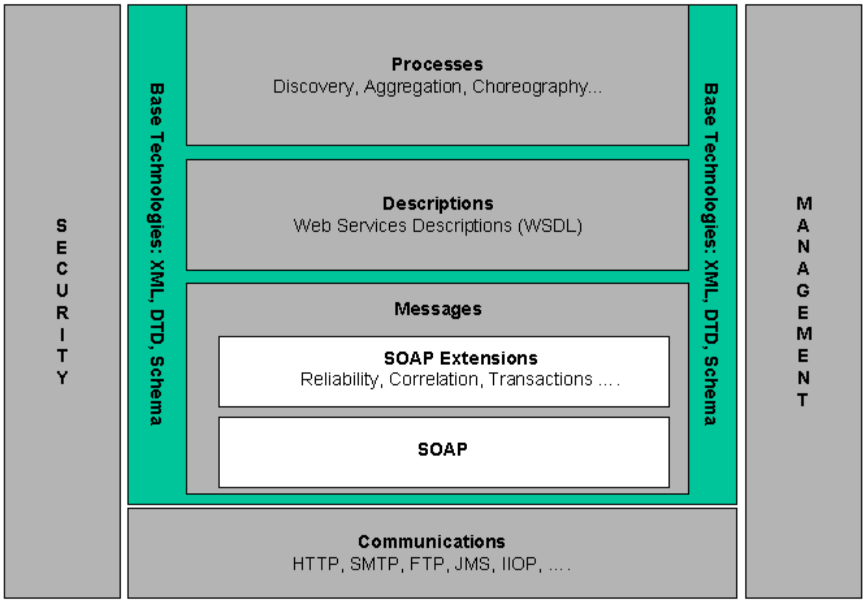

SECURITY
Base Technologies: XML, DTD, Schema
Processes
Discovery, Aggregation, Choreography...
Descriptions
Web Services Descriptions (WSDL)
Messages
SOAP Extensions
Reliability, Correlation, Transactions ....
SOAP
Base Technologies: XML, DTD, Schema
MANAGEMENT
Communications
HTTP, SMTP, FTP, JMS, IIOP, ...

Figure 5.2 Conceptual Web Services Architecture Stack

4.2 ESM Technology/Solutions

The ESM technology/solutions can be divided into two primary categories: On-line and Off-line. On-line functions provide near-real-time management of specific operational resources. Off-line functions support planning, analysis, and support functions that are less time critical.

4.2.1 On-line Functions

SNMP Core Framework - The Core Framework or SNMP Management Core provides the basic management console for topology display; the SNMP engine for polling and setting MIB objects, trap generation, logging functionality; the basic management data repository and the foundation for the integration of other tools. The core framework also includes the Manager-to-Manager (M2M) Interface capability for the EMS to allow data exchange with other management systems in a standard way.

Network Management - Network Management provides the ability to monitor and control network interconnect devices. Monitoring includes the collection and storage of key device parameters. Controlling includes the ability to affect the configuration of the device. The data that is collected will support the analysis of network traffic (availability, utilization, capacity, errors, and throughput) and the generation of associated network performance profiles.

Host / Device Management - Host Management provides the capability to monitor, display, detect, set, and report information about computer hosts and peripheral devices. Host parameters include accessibility, CPU usage, memory usage, swap usage, and disk usage. Device Management provides the capability to monitor and control other SNMP and non-SNMP devices connected to the enterprise network.

Application Management - Application Management provides the capability to monitor and control software application processes on monitored computer hosts. In addition, to the collection and display of application parameters (performance, space, resource conditions, availability), application management allows for the initiation and termination of application software directly from the management console.

Security Management – Security Management provides the capability to manage user and network security across a distributed environment. User security includes the management of available authorization and authentication controls. Network security includes the ability to protect the managed environment from specific external accesses. Security Management may also provide capabilities for legal intercept support.

Fault Management – Fault Management provides the capability to detect, display, and report any failures or threshold violations for all system resources. In addition, Fault Management provides the necessary tools to support correction of the identified fault. Fault Management also provides the capability to correlate errors to support faster identification and resolution of related infrastructure / environment problems.

Facility Management – Facility Management provides the capability to monitor power, heating, and cooling systems utilized in the managed enterprise.

User Interface / Centralized Status Console – User Interface provides the user's view into the EMS System, this can include standard X Displays, Web Interfaces or other advanced approaches (e.g., web portals). Centralized Status Console provides a custom view, tailored to user-needs of the enterprise domain being managed. Centralized Status Console will also provide the capability to integrate status information from multiple management domains into a single view (Manager-to-Manager).

Internet Services Management – Internet Services management provides the capability to monitor web site availability, web page access ("hits"), e-mail traffic, ftp traffic, etc. Internet Services also support messaging and paging functionality.

4.2.2 Off-line Functions

Information System Analysis & Reporting Services – Information System (I/S) Analysis provides integrated tools to support trending and capacity planning for infrastructure resources. I/S Reporting provides the capability to generate formatted reports and displays of available management information in standard templates or user-defined formats. I/S Analysis & Reporting services also include modeling and simulation functions.

Problem / Change Management – Problem / Change Management provides the capability to support the tracking of infrastructure problems & enhancements. Problem Management also supports the creation and execution of defined work-flow procedures.

Hardware & Software Asset Management – Hardware & Software Asset Management provides the capability necessary to support the tracking of infrastructure resources including all hardware and software assets. Information includes physical location (host), building/room, owner, etc. In addition, Hardware & Software Asset Management provides the capability necessary to manage COTS Software Licenses & COTS Software Maintenance Contracts, distribute COTS Software, and maintain an accurate COTS Software Inventory.

Distributed System Administration – Distributed System Administration provides the capability to access O/S level tools from the EMS console and to integrate the resulting data with the EMS data repository. Distributed System Administration also supports the administration of time services, users accounts, directory services and other common infrastructure capabilities.

Database / Archive Management – Database / Archive Management provides the capability to store management data in a standard format. Flat files will be used for the basic architecture and databases (e.g., RDBMS) will be used for Intermediate and Advanced architectures. In addition, the database functionality will then allow for addition, retrieval, modification, search, and display of available data about any system resource. The Database / Archive Management function can also support the administrative interfaces required to provide backup/restore and archive of the associated data when it is moved off-line as well as providing statistical information related to database systems (usage, space requirements, backup status, quota management). Although nominally intended for management information, this function can also support the management and monitoring of non-management/operational data.

Service Level Management – Service Level Management provides the capability to ensure that service level agreements for end-users are satisfied. Service Level Management also provides the necessary billing and accounting services.

EMS Development Services – EMS Development Services provide the development tool kits necessary to customize the EMS COTS components.

4.2.2 Technology Map to Vendor Products

The vendor landscape for these technologies is extremely diverse. The table below shows examples of technologies and products that can be deployed to service the various functions.

EMS Function	Technologies and Products
SNMP Core Framework	HP OpenView (HPOV) NNM & Operations, IBM Tivoli, CA Unicenter, Sun Managament Center (MC), FreshWater, Concord eHealth, SNMP Agents, IETF RFC -based tools from SNMP Research
Network Management	HPOV, Agents, Cisco LMS, Vendor MIBs
Host/Device Mgmt	HPOV, Agents, Vendor MIBs, HP Insight Manager
Application Mgmt	HP Operations (templates), HP Smart Plug-In, Agents, Custom-developed APIs
Security Mgmt	NetRanger, CSPM, Cisco Secure, Tripwire, RSA, OPSEC Alliance
Fault Management	Seagate NerveCenter, Expert System products
Facility Management	HPOV, Liebert OnliNet, Carrier ComfortView, Veritas Nerve Center
I/S Analysis & Reporting Services	HP Reporter / HP Internet Services, Concord eHealth
Problem / Change Management	Remedy ARS, Remedy HelpDesk

Hardware & Software Asset Management	Peregrine Asset Manager, Novadigm, TIBCO Active Enterprise
Distributed System Management	Solstice Admin
Database/Archive Management	Oracle, SQL (Windows), Sybase, Ingres, HP DB SPI, Veritas, Legato, HP OmniBack
User Interface/Centralized Status Console	X, HTML, PlumTree, iPlanet, Data Channel, HP Service Information Portal, IBM WebSphere, Oracle Application Server, BEA WebLogic
Internet Services Management	Web Trends, HP Internet Services, Concord eHealth
EMS Development Services	HP Openview Development Toolkit

4.2.3 Futures

The future technologies in Enterprise Service Management are many, however there are a few key trends and technologies to watch over the next two to five years including; server provisioning and configuration management, web services management, UDDI, and real-time applications. These technologies will become very important over the next few years, especially for service based architectures.

Server provisioning and configuration management are tools that provide image management, auto-discovery of hardware and software assets, change and configuration management (including application updates, configuration settings, etc.), and dynamic provisioning (hardware or software virtualization).

Web Services Management is technologies like web services brokers and web services operations management tools. These tools manage the capacity, availability and performance of applications or platforms.

Universal Description, Discovery and Integration (UDDI) is a directory service that has the ability to integrate with enterprise management. UDDI will provide capabilities for services to register and then be managed by the ESM.

Real-time applications and infrastructure is a new concept that allows resources and technology to be made available to consumers of the service on an as needed basis. The model allows for an enterprise management system to distribute resources to meet service level agreements and resource demands.

5 ESM Issues and Recommendations

1. To many standards to follow, and risk on selecting a standard that will not survive and be supported by the COTS providers.
    a. Recommendation: Minimize risk - Wait for market/standards maturity. Select more then one standard to follow – No standard covers all elements of ESM. DISA must be proactive in standards bodies to mature standards and protect investment.
2. To manage end-to-end services to support the war-fighter, DISA's ESM will have to manager and possible command, IT assets that are not owned by DISA but are owned by individual armed forces, joint assets, IC assets and commercial assets.
    a. Recommendation: create a Governance model that will allow DISA to see and possible command IT assets that are key to the delivery of Network Centric services to the war-

fighter. To accomplish this, several items will be need including: MOUs between DISA and other parties, manager-to-manager interface capability, standards for product/capability integration, common data definition and a common EA for ESM across the GIG, business domains, war-fighter domains and IC domains

3. Current, legacy mission systems are not defined and manageable as an Enterprise Service. Defining and developing a complete configuration of all current, legacy service components that comprise a Mission Enterprise Service, can be time consuming and expensive.
    a. Recommendation: Minimize the number of current systems that the Gov retrofits just for ESM objectives. Focus only on key legacy systems and services that are not planned for near term replacement or upgrades. Retrofit system with ESM hooks during upgrades cycles. Require ESM hooks and compliancy to NCES EMS Integration Requirements for new DoD systems.

6 Recommendations

6.1 Near Term – Today

Recommend DISA build upon their current investment of network and system management tool with incremental changes to lay down the foundation of process, tools and best practices to address the long term goal of service based delivery of all war-fighter capabilities and future objectives of NCES. We recommend DISA consider the following:

- Adopt a standards based ESM framework that provides guiding principles for a service based management solution.
    - ITIL is a leading framework that could be adopted. (See Appendix B - ITIL Framework
    - DISA must participate with standards bodies
    - Establish an ESM service oriented architecture
- Enhance current Network Management and System Management capabilities in the direction of Service Level Management (SLM) and Quality of Service (QoS) solutions/capabilities
    - Define, monitor, manage and adjust the service levels and the quality of services/solutions that DISA currently delivers
        - Start with 8 NCES services
    - Initiate automated life cycle management process and tools of existing DISA assets and services
- Promote the creation of a governance ESM model with the owners of the IT services in the war-fighter domain, Business domains and Intel Community domain for real-time management of end to end DoD/IT Services.
    - Address “Fee for service” model, where the Services can get the best value or QoS model from DISA

6.2 Long Term – 5+ Years

- All war-fighter services managed end to end as a service, not as IT parts of systems.
    - Global ESM view of all services supporting the war-fighter
- Fully integrated ESM and Security Management (IA) services

- Automated life cycle management of NCES
- Retire and replace systems that are not manageable or comply with a service based management architecture
- Global view of all services for all domains and community of interest from a single (and distributed) management center.
- Real time (immediate) ability to control the QoS of all services supporting the warfighter.

Appendix A - Terms

Ad-Hoc COI – an operational COI that forms in response to immediate events. Ad-hoc COIs come into existence to address an issues and disband once that issue have been resolved.

Application Schema – An application schema provides the formal description of the data structure and content required by one or more information communities. --- set of conceptual schema for data required by one or more applications.

COI – Community of Interest.

DCP – Distributed Computing Platform

F**eature** – abstraction of a real world phenomenon or attribute of a system

Federation – an IT configuration where organizations and systems collaborate without a single management framework.

GML – Geographic Markup Language

Information Community - a collection of people (a government agency or group of agencies, a profession, a group of researchers in the same discipline, corporate partners cooperating on a project, etc.) who, at least part of the time, share a common digital geographic information language and common spatial feature definitions.

Interface – named set of operations that characterize the behavior of an entity

Jurisdiction - an administrative entity with a single management authority that can establish standard policies, procedures, and technologies. All systems within a jurisdiction are subject to this management framework.

Metadata – data about data.

OGC – Open GIS Consortium

Ontology – the working model of entities and interactions in some particular domain of knowledge or practices, such as electronic commerce or "the activity of planning." A set of concepts - such as things, events, and relations - that are specified in some way (such as specific natural language) in order to create an agreed-upon vocabulary for exchanging information In artificial intelligence (**AI**), an ontology is, according to Tom Gruber, an AI specialist at Stanford University, "the specification of conceptualizations, used to help programs and humans share knowledge." . One or more taxonomies can be developed for the ontology and taxonomies can be used as part of the ontology model.

Operation – specification of a transformation or query that an object may be called to execute. Also, a virtual enterprise established to achieve some real world goal (e.g., Operation Iraqi Freedom) – see Ad Hoc COI

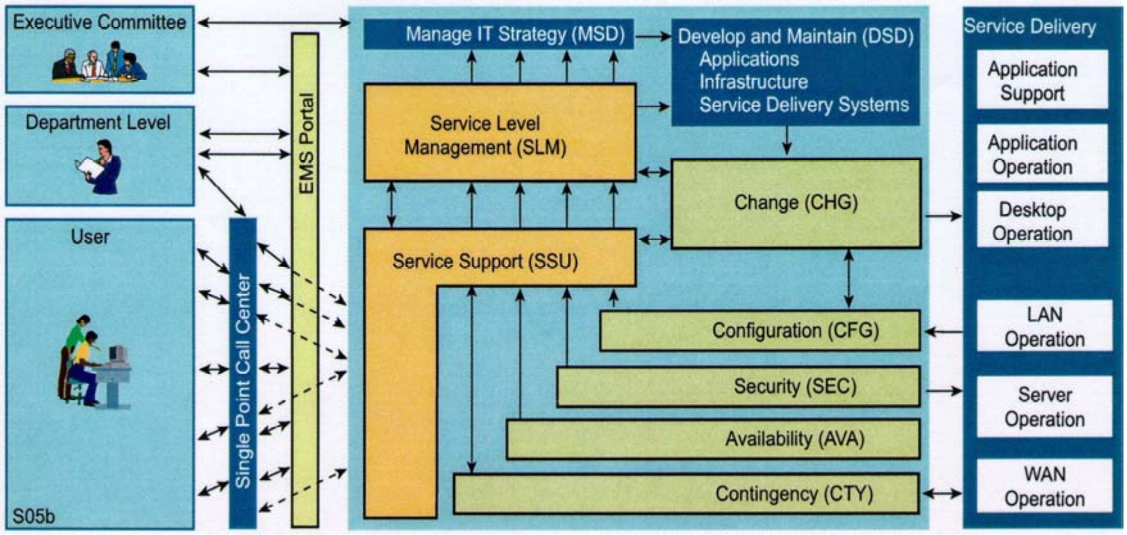
Operational COI - a collection of individuals, organizations, and systems with similar business and information needs. Operational COIs operate across Jurisdictions and Federations and in fact are the primary reason for their existence. Operational COIs develop their own operating conventions addressing such issues as information models, policies, and practices.

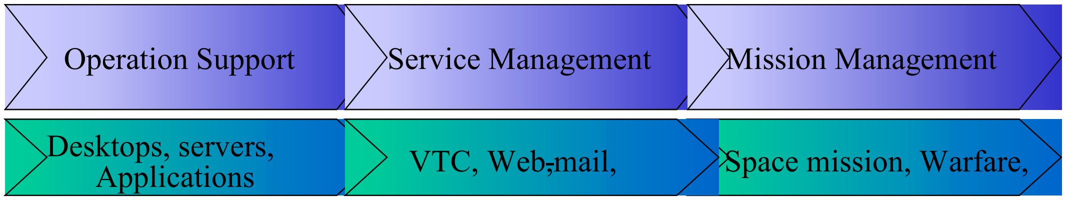
Service – distinct part of functionality that is provided by an entity through interfaces accessible over the GIG network.

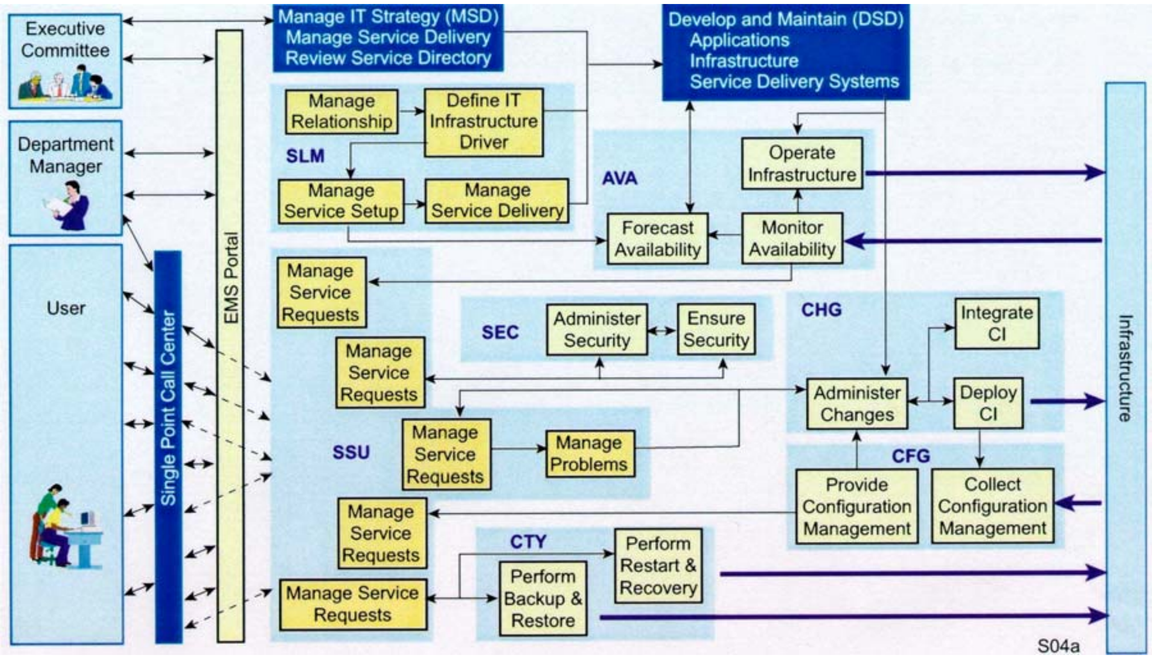
Taxonomy – the science of classification according to a pre-determined system, with the resulting catalog used to provide a conceptual framework for discussion, analysis, or information retrieval. In theory, the development of a good taxonomy takes into account the importance of separating elements of a group (taxon) into subgroups (taxa) that are mutually exclusive, unambiguous, and taken together, include all possibilities. In practice, a good taxonomy should be simple, easy to remember, and easy to use. However most real world entities and concepts can be viewed as belonging to multiple taxonomies, based on the operational context in which they are referenced. For example, a main battle tank is both a vehicle and a weapon system. It can also be a shelter, cargo, asset, target, etc. in other operational contexts and thus taxonomies.

Viewpoint – form of abstraction achieved using a selected set of architectural concepts and operational contexts with associated structuring/representation rules, in order to focus on particular concerns within a system development, acquisition, or virtual enterprise context.

Appendix B – ITIL Framework


Executive Committee
Department Level
User
S05b
Single Point Call Center
EMS Portal
Manage IT Strategy (MSD)
Develop and Maintain (DSD)
Applications
Infrastructure
Service Delivery Systems
Service Level Management (SLM)
Change (CHG)
Service Support (SSU)
Configuration (CFG)
Security (SEC)
Availability (AVA)
Contingency (CTY)
Service Delivery
Application Support
Application Operation
Desktop Operation
LAN Operation
Server Operation
WAN Operation


Operation Support
Service Management
Mission Management
Desktops, servers, Applications
VTC, Web,mail,
Space mission, Warfare,


Executive Committee
Department Manager
User
Single Point Call Center
EMS Portal
Manage IT Strategy (MSD)
Manage Service Delivery
Review Service Directory
Develop and Maintain (DSD)
Applications
Infrastructure
Service Delivery Systems
Manage Relationship
Define IT Infrastructure Driver
SLM
Manage Service Setup
Manage Service Delivery
AVA
Operate Infrastructure
Forecast Availability
Monitor Availability
Manage Service Requests
SEC
Administer Security
Ensure Security
CHG
Integrate CI
Manage Service Requests
Administer Changes
Deploy CI
SSU
Manage Service Requests
Manage Problems
CFG
Manage Service Requests
Provide Configuration Management
Collect Configuration Management
CTY
Perform Restart & Recovery
Manage Service Requests
Perform Backup & Restore
Infrastructure
S04a