|  |
| --- |
| Army Cost Benefit Analysis: **DoD E-mail Services[[1]](#footnote-1)** |
|  |
| Army Chief Information Officer/G-6  |



Contents

[Executive Summary 2](#_Toc327359918)

[1. Definition of the Problem/Opportunity 3](#_Toc327359919)

[a. Problem Statement 3](#_Toc327359920)

[b. Background 3](#_Toc327359921)

[c. Current State 4](#_Toc327359922)

[d. Objective 5](#_Toc327359923)

[2. Research 6](#_Toc327359924)

[3. Definition of Scope, Facts and Assumptions 9](#_Toc327359927)

[a. Scope 9](#_Toc327359928)

[b. Facts 9](#_Toc327359929)

[c. Ground Rules 9](#_Toc327359930)

[d. Assumptions: 10](#_Toc327359931)

[e. Constraints: 10](#_Toc327359932)

[Appendix A 11](#_Toc327359933)

[Appendix B 12](#_Toc327359934)

# Executive Summary

The Army continuously expands its use of information technology products and services to perform its mission and conduct business. However, the Army’s IT systems are extremely segmented, presenting several major significant concerns that put the Army's effectiveness at risk. The issues that exist within the current state of the Army IT infrastructure prevent the user community from effectively and securely sharing information and collaborating in a timely manner. As a result of this fractured state, the Army's security posture is inconsistent and unpredictable, and it causes the system to be needlessly expensive to operate and maintain.

The Army recognized these challenges and inefficiencies and has directed the Office of the Army Chief Information Officer (CIO/G-6) to develop a strategy to address a global consolidation effort of disparate IT services and resources. In addition, the establishment of a single DOD enterprise is a concept called for by DOD CIO and the DOD Enterprise Guidance Board (EGB), and endorsed by the Secretary of Defense. Another factor is that the White House, through the U.S. CIO and the Office of Management and Budget (OMB) has directed that all Federal agencies, including the military departments, to comply with the Federal Data Center Consolidation Initiative (FDCCI). The Vice Chief of Staff, Army (VCSA) issued clear guidance during the 2010 ADCCP Capability Portfolio Reviews to execute data center consolidation beginning in FY11 with a specific target of a 75 percent reduction in Army data centers within five years to gain efficiencies, improve performance and increase security.

The Army E-mail initiative seeks to fully support the OMB, DOD, and Army mandates through the consolidation and rationalization of segmented E-mail systems on differing platforms, including Sun's (acquired by Oracle) Java Communication Suite (JCS) and Microsoft's Exchange Server. While the Sun JCS system is centralized in the form of AKO, the Microsoft Exchange platforms are globally distributed across the Army. The current systems are managed and deployed separately reducing collaborative capabilities and increasing the cost by having duplicate systems.

# Definition of the Problem/Opportunity

|  |
| --- |
| **Summary** |
| *Redundant E-mail capabilities, including the centralized AKO, and between 18 and 25 disparate Exchange systems across the globe, along with the high number of servers and personnel required to maintain them over the lifecycle of the systems, lead to high costs and significantly hindered collaboration capability across the Army.* |

## Problem Statement

Redundant E-mail capabilities, including the centralized AKO and over eighteen Exchange systems across the globe, along with the high number of servers and personnel required to maintain them over the lifecycle of the systems, lead to high costs and significant operational inefficiencies across the Army. The Army has been managing IT services such as E-mail as separate, disparate entities for a number of years. However, the ability to share calendars, information, and more has become an enterprise requirement necessary to provide the resources and services for Army user communities and operational missions. The establishment of a single DOD enterprise is a concept called for by DOD CIO and the DOD Enterprise Guidance Board (EGB), and endorsed by the Vice Chairman of the Joint Chiefs of Staff (VCJCS). The Army’s current IT environment consists of a minimum of eighteen Microsoft (MS) Active Directory forests each running their own instance of Microsoft’s Exchange messaging system. Additionally, AKO hosts a Sun Java Communication Suite (JCS) E-mail service. This results in a second, duplicate mailbox for every Army user. This presents an unnecessary duplication in costs to the Army. Most Army installations host their own MS Exchange servers along with the accompanying support staff. This separation of service causes a number of capability gaps and operational risks for the Army:

* 1. Lack of calendar sharing across organizations
	2. Lack of delegation to users in other organizations
	3. Inefficiencies as soldiers transfer between duty stations
	4. Duplicate services deployed throughout the Army
	5. Duplicate administration responsibilities
	6. Underutilized hardware
	7. Potential security vulnerabilities due to multiple disparate authentication mechanisms, including username/password
	8. Lack of COOP capability
	9. Non-conformance with requirements to journal specific E-mail messages

## Background

The Army spends a disproportionate amount of money managing its current segmented E-mail systems (between 18 and 25 in total) on differing platforms, including Sun JCS and MS Exchange Server. In 2007 Gartner provided the Army CIO G-6 E-mail Study (221496830) - Analysis and Recommendations Brief - 20 Nov 07, stating that the Army should consolidate its segmented Exchange resources into a single collaborative system.

1. In 2008 the Department of Defense started exploring the idea of creating a single DOD-wide E-mail solution. A Tiger Team was assembled to determine which product should be used to provide a consolidated E-mail solution for the Army/DOD. This team did a comprehensive product comparison between Sun JCS, Yahoo Zimbra (now owned by VMWare), and MS Exchange. Based on a weighted analysis, the team recommended that Microsoft (MS) Exchange Server be used as the product of choice for the DOD-wide consolidated E-mail solution strategy. Studies performed by Gartner and MITRE support the team’s scalability and feasibility findings, as well as being able to achieve the objective to reduce the overall DOD cost to manage E-mail and provide a global collaborative service.
2. On 26 February 2010, the Office of Management and Budget (OMB) directed that all Federal agencies, including the military departments, comply with the Federal Data Center Consolidation Initiative (FDCCI).
3. The Vice Chief of Staff, Army (VCSA) issued clear guidance during the 2010 ADCCP Capability Portfolio Reviews to execute data center consolidation beginning in FY11 with a specific target of a 75 percent reduction in Army data centers within five years to gain efficiencies improve performance and increase security.
4. The Army E-mail initiative seeks to fully support the OMB and Army mandates through the consolidation and rationalization of its E-mail systems.

# Current State

Today, the Army manages its E-mail services in a segmented fashion with Army organizations hosting over eighteen different E-mail systems running Microsoft Exchange and one solution running Sun JCS. All of these efforts are currently funded as independent groups of IT services. They do not provide the required Net-Centric capability, nor do they meet the strategic objectives of the Army’s Global Network Enterprise Construct strategy. The stove-piped systems can lead to great inefficiencies, and can hinder collaboration across organizations and with our joint mission partners.

The current multiple platforms, by their design, consume valuable resources, owing to the segmentation of administrative functions and the separation of users into two groups, many of whom must manage two E-mail addresses and accounts. While one could argue that the multitude of Army organizations running independent E-mail services could be of benefit in the face of a cyber-event (i.e., if one system is compromised, others could function normally, given they’re not interdependent), this ignores the more significant security issues posed by the number of security vulnerabilities resulting from the stove-piped systems. Furthermore, the current E-mail infrastructure is a barrier to supporting the highly-mobile, connected war fighter of the future.

With the current E-mail (and calendar and directory) environment comprised of multiple platforms, products and disparate processes, people cannot view calendars or look up addresses across organizational lines. The Army is currently paying multiple times for the same service with AKO’s Sun JCS and the locally run Microsoft Exchange systems. There is little opportunity to optimize storage solutions, and the status quo results in E-mail being hosted at multiple locations on many Army installations, since the systems are segmented along organizational lines. Cost reduction is not feasible maintaining a non-integrated set of E-mail delivery systems that require unnecessary network and systems administrative overhead. From an information assurance (IA) perspective, there are significant risks associated with keeping the As-Is environment. There are potential security threats due to the lack of a single security policy. Additionally, security enhancements that would be realized by moving to more modern versions of hardware and software (for example, 64 vice 32-bit server systems, Exchange 2010 vice Exchange 2003) are delayed due to the high cost and complexity of implementing upgrades across multiple organizations and systems. While the Army enjoys total control over its current E-mail infrastructure, the lack of a centralized administrative control function or processing center(s) can lead to disparate controls being enacted by each mail system. This lack of consistency leads to inconsistent implementation of policy guidance, and increases the difficulty in responding to security incident in a timely manner. The availability of E-mail service would neither become better nor worse, but simply remain the same due to no change in the existing systems.

# Objective

The goal is to provide the Army with a single E-mail solution that will unify the disparate messaging systems of today and allow for a single directory service and increased collaboration amongst the Army community. This consolidated system will allow the Army to eventually retire the duplicate E-mail services and eliminate the redundant costs to the Army providing a significant cost savings. In addition, the establishment of a single DOD enterprise is a concept called for by DOD CIO and the DOD Enterprise Guidance Board (EGB), and endorsed by the Secretary of Defense.

Come up with 3 alternatives not including the status quo. The specific objectives of Army E-mail include:

1. Facilitate the seamless movement of Army users between organizations. Provide a centralized Army solution for E-mail, calendaring, and directory services
2. Reduce information technology costs,
3. Increase security of the global enterprise network
4. Conform to enterprise architectural standards. Increase management control over resource execution and performance
5. Allow access to E-mail from any location

# Research

##

At an Information Technology seminar, Mr. Ernest Johnson approaches you with capabilities available from his company, Google.

An Army Email Service System hosted by Google would provide the Army with a single E-mail solution that collapses the messaging systems of today into a single managed E-mail organization. This consolidated system will allow the Army to remove the duplicate E-mail services and costs to the Army. This would reduce the number of server licenses, the amount of hardware required, provide central management functions, and enhance the collaborative capabilities of Army E-mail users, as well as significantly larger mailboxes.

Moving toward a hosted, single E-mail infrastructure offers significant benefits in the areas of user functionality, administration and security. E-mail standardization helps the Army overcome the variations in technical processes and policy implementation present at the installation level and also helps them apply industry-standard E-mail best practices across the Army Enterprise. The Army substantially improves its global collaborative capabilities, both within the Army and with its mission partners. This helps bridge the divide between deployed and garrison soldiers, given they would share a common user interface and back-end. From an architecture view, the Army stands to realize cost reductions due to an overall reduction in the number of E-mail servers, hubs and domain controllers, and the related duplicative administrative overhead to run and maintain them all.

The commercial provider would still have the same requirements as government for physical security, network security, contingency operations, and system integration that is provided at a government facility. Once the government has made an initial investment in a commercial vendor, it could be costly to move to another vendor in the future.

The commercially managed infrastructure provides universal access to E-mail from multiple devices and methods of delivery. This enterprise system facilitates integrated access and storage of E-mail, meetings and workflow/task management activities across the Army. There would also be a single, comprehensive Global Address List available to all Army users. With a commercially hosted Army E-mail system, the Army achieves significant cost reductions by reducing its geographic footprint and centralizing its system. In doing so, they would move away from the current model of multiple platforms and processes and have the benefit of aggregation of services and functionality. This would translate into the elimination of excessive and redundant hardware, licensing, administration and configuration costs. The Army’s security posture will be greatly enhanced, in that a commercially hosted solution will have to adhere to Army requirements for security compliance with DOD disaster recovery policy and continuity of operations policy (DR/COOP). By moving to a commercially hosted architecture, the Army would no longer be encumbered with the IA vulnerabilities inherent with multiple, disparate systems, products and processes. This will greatly improve the security posture of E-mail services compared to the current separate systems. There is a possibility that a commercial provider could have a steeper learning curve for the implementation and use of mandatory DISA supplied security templates. While the Army admittedly cedes control over its Army E-mail infrastructure, it will benefit from the centralized administration and support model, where there will be standardization of hardware and software and accompanying configuration control. The corresponding reduction in the number of hardware and software configurations will allow the commercial provider to simplify its C2 model while at the same time offering the Army increased reliability and availability of E-mail resources. The availability of E-mail service would be greatly enhanced, based on the fact that the commercial provider data centers are compliant with DOD disaster recovery policy and continuity of operations policy (DR/COOP). However, as there are fewer geographic locations for hosting mail; therefore, any incident at one location has the potential to disrupt a larger number of users.

One advantage of using a commercial service provider is the lower risk in future contracts. With the size of the Army and the size of the civilian workforce constantly being threatened with RIFs, Google would be able to accommodate these changes – offer more flexibility in the case of a smaller force, so that the Army would not have to pay for mailboxes they were not using.

##

Through COL Smith of the Cyber command, you have been introduced to Ada Jones, of DISA. Her recommendation is, surprisingly, to use DISA as a hosting solution.

DISA is already in the business of providing secure, scalable IT solutions to DOD customers. It already possesses the processes and technical depth for hosting Army and other DOD applications, as well as a global network of enclaves for hosting applications such as E-mail services. The DOD E-mail service would be hosted at 9 Defense Enterprise Computing Centers (DECCs), 7 in the Continental US, 2 overseas, “mini-Pods” of servers located at geographically disadvantaged locations or high concentrations of critical users to assure performance and availability through automated failover mechanisms. The DECCs enjoy essentially unlimited bandwidth by being directly connected to a robust and geographically redundant DOD-owned fiber optic cable backbone.

Moving toward a hosted, single E-mail infrastructure offers significant benefits in the areas of user functionality, administration and security. E-mail standardization will enable the Army to overcome the variations in technical processes and policy implementation present at the installation level and also apply industry-standard E-mail best practices throughout the Army Enterprise. The Army would be substantially improving its global collaborative capabilities, both within the Army and with its mission partners. This will help bridge the divide between deployed and garrison soldiers, given they would share a common user interface and back-end. Architecturally, the Army should stand to realize cost reduction owing to an overall reduction in the number of E-mail servers, hubs and domain controllers, and the related duplicative administrative overhead to run and maintain them all.

The DISA managed infrastructure provides universal access to E-mail from multiple devices and methods of delivery. This enterprise system facilitates integrated access and storage of E-mail, meetings and workflow/task management activities across the Army. There would also be a single, comprehensive Global Address List for the entire DOD available to all Army users, enhancing the collaborative capabilities of Army E-mail users, and DOD users as well. With a DISA hosted Army E-mail system, the Army achieves significant cost reductions by reducing its geographic footprint and centralizing its system under DISA stewardship. In doing so, they would move away from the current model of multiple platforms and processes and have the benefit of aggregation of services and functionality. This would translate into the elimination of excessive and redundant hardware, administration and configuration costs. The army could reduce the number of server licenses, amount of hardware required, and provide central management functions.The Army’s security posture would be greatly enhanced, in that DISA’s data centers are secure and compliant with DOD disaster recovery policy and continuity of operations policy (DR/COOP). By moving to a DISA hosted architecture, the Army would no longer be encumbered with the IA vulnerabilities inherent with multiple, disparate systems, products and processes. DISA rigorously enforces a standard security configuration, allowing for limited, mitigated variances. This will greatly improve the security posture of E-mail services compared to the current separate systems. Additionally, since DISA is the authority for security templates applied to servers, they are uniquely able to deploy security templates and guidance to the messaging infrastructure. The Army will benefit from the centralized administration and support model, where there will be standardization of hardware and software and accompanying configuration control. The corresponding reduction in the number of hardware and software configurations will allow DISA to simplify its C2 model while at the same time offering the Army increased reliability and availability of E-mail resources. The availability of E-mail service would be greatly enhanced, on the assumption that DISA’s data centers are compliant with DOD disaster recovery policy and continuity of operations policy (DR/COOP). However, there are fewer geographic locations hosting E-mail in the DISA hosting alternative. Any incident at one facility has the potential to affect a greater number of users than the status quo. This risk is mitigated as the DISA alternative complies with MAC II requirements for DR/COOP.

# Definition of Scope, Facts and Assumptions

## Scope

1. Army E-mail is intended to provide users across the DOD (and eventually the Intelligence Community (IC)) an integrated solution for electronic mail, shared calendaring, directory, and an Outlook desktop client, a web client and/or a mobile device client as well as Blackberry Enterprise Server (BES) for selected users.
2. The threshold capability of Army E-mail is a subset of the functions listed above for the entire US Army user population and possibly some other government entities. Requirements were gathered from the USA, USAF, USN, USMC, TRANSCOM, DISA, OSD, and SOCOM.
3. Army E-mail will provide E-mail and calendaring for all Army CAC card holders on NIPRNET (approximately 1.4 million users) and 200,000 SIPRNET users.
4. Family, Friends and Retirees are not part of the scope of Army E-mail
5. Tactical systems are not part of the scope of Army E-mail at this time.

## Facts

 There are a total of 1.6M mailboxes consisting of:

1. 900K NIPR “business” mailboxes
	1. 800K individual user mailboxes, for which the Army has adequate user licenses for those individuals who login to a DOD computer and use E-mail daily as part of their job.
	2. 100K organizational mailboxes, which do not require user licenses
2. 500K NIPR Webmail user mailboxes for individuals do not use E-mail as part of their daily job
3. 200K SIPR mailboxes

## Ground Rules

1. 4GB mailboxes for business users
2. 500MB mailboxes for Webmail users
3. The Army E-mail service provider:
	1. Provides Tier 2/3 services
	2. Implements, accredits, and operates Army E-mail
4. Base Year is FY11
5. Period of Estimate is FY11-FY17
6. All users will migrate in CY11
7. Journaling will be supported for 3% of users for 7 years (To-Be COAs)
8. Hardware lifecycle replacement is 5 years
9. Army E-mail must be operated IAW MAC II policies
10. Authentication of Army E-mail will be performed using CAC PKI certificate (No User Name and Password).
11. NetOps cost incurred by NETCOM are excluded
12. BlackBerry device and data plan cost are excluded
13. Costs of existing (As-Is) solution's disposal of existing equipment, reassignment of personnel , and changes in support contracts are excluded

## Assumptions:

1. The Managed Service Provider (MSP) will have to acquire all server-side software licenses and hardware equipment.
2. The Army will have to acquire 500K client access licenses from Microsoft for the NIPR Webmail users to use with MS Exchange.
3. The Army will continue to provide centralized message filtering after all users are moved to the MSP, for “defense in depth”. This leads to filtering costs being added to the To-Be estimates.
4. Tier 1 service is included in Army Enterprise Service Desk and by Network Enterprise Centers
5. Additional bandwidth requirements at local posts/camps/stations are not significantly different across the alternatives

## Constraints:

1. Army E-mail service will migrate before data centers are closed by the Army Data Center Consolidation Project (ADCCP).
2. Achieve cost savings per 16 Aug 2010 – DOD IT Efficiencies Initiative - “Consolidate DOD IT infrastructure to achieve greater economies of scale”).
3. The MSPs must be able to meet the constraint in the Requirements Specification to use government data centers.
4. The MSPs will use Microsoft Exchange 2010 as the server product.

Users will be provided the same or better service.

# Appendix A

Baseline cost estimates:

Network Enterprise Centers (NEC) typically are funded through multiple sources, including charges to tenants for direct costs incurred. Examples of costs that are typically not charged include costs of government staff and facilities (space, power, and bandwidth). The data collected was normalized for the required storage, number of BlackBerry users, and costs of facilities. However, these normalized costs are still understated as some costs such as management overhead and government labor are not taken into account.

The figure below compares the costs at the three installations. Two costs are shown for both FT Belvoir and Redstone; one for 1 GB mail storage and another with the full 2.7 GB storage/archive.

The total cost of the Status Quo also includes the cost of AKO. AKO costs $20.1 (FY11$M) per year.

Inflation indices can be found on the ASA FM&C website.

# Appendix B

The investment and recurring costs for a commercial managed service provider (MSP) have been estimated, based on the Ground Rules & Assumptions listed in an earlier section, and additional key assumptions listed below:

1. Labor costs are based on ITES-2S Contract
2. Equipment prices are based on ITES-2H, GSA, and commercial quotes in that order
3. Storage costs are assumed to reduce 15% per year (based on industry trends and AKO data of 15% annual reduction)
4. Storage and Archiving build up over 2 year period
5. DR/COOP requires:
	1. 2 CONUS data centers with TLA equipment for security at both sites (primary & COOP)
	2. 1:1 equipment redundancy
	3. Bandwidth for COOP data replications - commercial WAN link

(not DISN) 2x Dual OC-48 from each data center

1. The MSP will have to acquire licenses (OS, Exchange).
2. The profit of the MSP is equivalent to a 6% fee
3. Journaling software is not required since it will use the capability available in Exchange 2010
4. Message Rates per day:
5. Business Users - 20 Transmit / 80 Receive
6. Webmail Users - 5 Transmit / 20 Receive
7. Average message size is 88KB, based on current AKO daily usage
8. Storage per user will be split into a higher tier for 1 GB , remainder will use a

 lower tier

1. NIPR and SIPR user costs are the same

In addition, contracting office and MSP contract closeout costs are excluded from the

Estimate.

The MSP has stated that the non-Business users (OWA) will need licenses to access Army E-mail. The cost of the perpetual client access licenses (CALs) has been added to the cost estimate and shown in the table below.

The table below provides the detailed cost estimate of this COA. It is expected that the

MSP will smooth out the Investment and Operations & Support costs in the price per user.

|  |  |  |  |
| --- | --- | --- | --- |
| Costs are in Base Year FY11 $M (Constant Dollars) | **MSP Estimate with Additional CALS** |  |  |
| **CE#** | **Cost Elements** | **FY11** | **FY12** | **FY13** | **FY14** | **FY15** | **FY16** | **FY17** |
| **1** | **Investment** | **$146.7** | **$15.3** | **$0.5** | **$0.7** | **$0.8** | **$27.1** | **$7.7** |
| **1.1** | **Program Management** | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 |
| **1.2** | **Concept Exploration** | $0.4 | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 |
| **1.3** | **System Development** | $2.1 | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 |
| **1.4** | **System Procurement** | $56.4 | $14.8 | $0.5 | $0.7 | $0.8 | $1.0 | $1.2 |
| **1.5** | **Outsource/Central/Mega Center Investment** |   |   |   |   |   |   |   |
| **1.6** | **System Initiation, Implementation & Fielding** | $32.2 | $0.6 | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 |
| **1.7** | **Upgrade P3I** | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 | $26.1 | $6.5 |
| **1.8** | **Disposal/Reuse** |   |   |   |   |   |   |   |
| **1.9** | **Client Access Licenses (CALs)** | $55.8 |   |   |   |   |   |   |
| **2** | **SYSTEM OPS & SPT** | **$29.1** | **$51.2** | **$51.0** | **$57.5** | **$57.0** | **$49.6** | **$49.3** |
| **2.1** | **System/Material/Item Mgmt** | $6.4 | $7.6 | $7.6 | $8.0 | $8.0 | $7.6 | $7.5 |
| **2.2** | **Annual Operations Investment** | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 | $0.0 |
| **2.3** | **Hardware Maintenance** | $0.2 | $0.2 | $0.2 | $6.8 | $6.8 | $0.2 | $0.2 |
| **2.4** | **Software Maintenance** | $3.3 | $10.3 | $10.3 | $10.3 | $10.3 | $10.3 | $10.3 |
| **2.5** | **Mega Center Ops & Maint Spt** | $0.2 | $0.2 | $0.2 | $0.2 | $0.2 | $0.2 | $0.2 |
| **2.6** | **Data Maintenance** |   |   |   |   |   |   |   |
| **2.7** | **Unit/Site Operations** | $19.0 | $32.9 | $32.7 | $32.2 | $31.8 | $31.4 | $31.1 |
| **2.8** | **Env & Haz Mat Store & Hand** |   |   |   |   |   |   |   |
| **2.9** | **Contract Leasing** |   |   |   |   |   |   |   |
|  |  |  |  |  |  |  |  |  |
|  | **Annual Cost per Mailbox ($)** | **$110** | **$42** | **$32** | **$36** | **$36** | **$48** | **$36** |

Estimates provided by this MSP have been misleading in the past. The following uncertainties apply:

1. 10% increase in labor rates increases the estimate by $2
2. 10% decrease in storage costs reduces the estimate by $1
3. 50% decrease in the number of racks due to use of blade servers & higher density storage reduces the estimate by $1
4. 20% reduction in software costs due to quantity software discounts from GSA prices reduces the estimate by $2
5. A Contract Office Fee of 1.5% increases the estimate by $1

The DISA Cost Estimate, based on the Ground Rules & Assumptions listed in an earlier section is shown below.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DISA: | Costs in BY11 $M |  |  |  |  |  |  |  |
| **CE#** | **Cost Elements** | **FY11** | **FY12** | **FY13** | **FY14** | **FY15** | **FY16** | **FY17** |
| **1.0** | **Investment** | **$84.485** | **$4.017** | **$4.106** | **$4.187** | **$4.270** | **$4.371** | **$4.475** |
| **1.1** | **Program Management** | $3.0 | $2.0 | $2.1 | $2.1 | $2.1 | $2.2 | $2.2 |
| **1.2** | **Email Data Migration** | $10.8 |   |   |   |   |   |   |
| **1.3** | **Blackberry Data Migration** | $4.0 |   |   |   |   |   |   |
| **1.4** | **SIPRNet** | $7.7 |   |   |   |   |   |   |
| **1.5** | **Outsource/Central/Mega Center Investment** |   |   |   |   |   |   |   |
| **1.6** | **System Initiation, Implementation & Fielding** |  |  |  |  |  |  |  |
| **1.7** | **Upgrade P3I** |   |   |   |   |   |   |   |
| **1.8** | **Server Licenses** | $0.2 |   |   |   |   |   |   |
| **1.9** | **Client Access Licenses (CALs)** | $55.8 |   |   |   |   |   |   |
| **2.0** | **SYSTEM OPS & SPT** | **$102.1** | **$97.8** | **$94.2** | **$91.0** | **$88.3** | **$86.1** | **$84.2** |
| **2.1** | **System/Material/Item Mgmt** | $11.0 | $11.1 | $11.4 | $11.7 | $12.0 | $12.3 | $12.6 |
| **2.2** | **Annual Operations Investment** |   |   |   |   |   |   |   |
| **2.3** | **Hardware Maintenance** | $34.8 | $32.4 | $30.2 | $28.3 | $26.6 | $25.0 | $23.7 |
| **2.4** | **Software Maintenance** | $5.2 | $5.3 | $5.4 | $5.5 | $5.6 | $5.7 | $5.8 |
| **2.5** | **Mega Center Ops & Maint Spt** |  |  |  |  |  |  |  |
| **2.6** | **Data Maintenance** |   |   |   |   |   |   |   |
| **2.7** | **Unit/Site Operations** |   |   |   |   |   |   |   |
| **2.8** | **Env & Haz Mat Store & Hand** |   |   |   |   |   |   |   |
| **2.9** | **Contract Leasing** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | Annual Cost per Mailbox ($) | 116.62 | 31.81 | 30.72 | 29.75 | 28.92 | 28.26 | 27.71 |

1. All Concepts and proposals in this case study are notional and for educational purposes only. They are not indicative of current or historical Army force design plans. The data should not be used for actual analysis outside of the classroom exercise. [↑](#footnote-ref-1)