



USAID
FROM THE AMERICAN PEOPLE

TAPRII
TECHNICAL ASSISTANCE
FOR POLICY REFORM

EGYPTIAN CUSTOMS STRATEGIC IT SECURITY- INFRASTRUCTURE ANALYSIS AND RECOMMENDATIONS

Egypt TAPR-II: Trade Component

June 22, 2006

This publication was produced for review by the United States Agency for International Development. It was prepared by Keith R. Worfolk.

EGYPTIAN CUSTOMS STRATEGIC IT SECURITY- INFRASTRUCTURE ANALYSIS AND RECOMMENDATIONS

EGYPT TAPR-II: TRADE COMPONENT

TECHNICAL ASSISTANCE FOR POLICY REFORM II

CONTRACT NUMBER: 263-C-00-05-00063-00

BEARINGPOINT, INC.

USAID/EGYPT POLICY AND PRIVATE SECTOR OFFICE

JUNE 22, 2006

AUTHOR: KEITH R. WORFOLK

SO 16

DISCLAIMER:

The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

CONTENTS

1. INTRODUCTION	3
1.1. Purpose	3
1.2. Objectives	3
1.3. Stakeholders	6
1.4. Scope	7
1.5. Constraints, Assumptions, and Dependencies	7
1.6. Approach	8
1.7. Approval Process	8
2. SECURITY AND IT INFRASTRUCTURE STRATEGIC END-STATE	9
2.1. Reference Architectures	9
2.2. Main Customs Sites Architecture Solution	9
2.3. Main Customs Sites Architectural Goals	11
2.4. Main Customs Sites Solution Overview	11
2.5. Secondary Customs Sites Architecture Solution	28
2.6. Secondary Customs Sites Architectural Goals	30
2.7. Secondary Customs Sites Solution Overview	30
3. OTHER ARCHITECTURAL CONSIDERATIONS	41
3.1. Developing a More Robust and Modern Enterprise Architecture	41
3.2. Addressing International Standards	42
3.3. Utilizing the Customs Data Interchange (CDI)	42
3.4. Upgrading the Database Management System (DBMS)	43
3.5. Launching and Maintaining a Data Warehouse	43
3.6. Establishing Regular and Automated Data Backup and Recovery	45
3.7. Establishing Enterprise Workflow Management	45
3.8. Establishing and Maintaining a Proper Website	46

3.9.	Creating a Single Window Environment for Customers	46
3.10.	Improving the Network Environment	47
3.11.	Improving Customs Technical Support	50
3.12.	Establishing and Maintaining IT Governance, Planning, and Support Services	53
3.13.	Instituting Enterprise-wide Antivirus Software	54
4.	OTHER CONSIDERATIONS	56
4.1.	Incorporating Risk Management	56
4.2.	Maintaining an IT Equipment Inventory	56
4.3.	Managing Software Licensing	56
4.4.	Managing Office Productivity Tools	57
4.5.	Maintaining the Customs Site Physical Environment	57
5.	NEXT STEPS	60
5.1.	Main Customs Processing Sites	60
5.2.	Secondary Customs Processing Sites	61
6.	SUMMARY OF KEY RECOMMENDATIONS	62
7.	EXAMPLE LIST OF PROJECT DELIVERABLES	69
8.	VENDOR EVALUATION CRITERIA	70
8.1.	Cost	70
8.2.	Product Specifications	70
8.3.	Installation, Warranty, Maintenance, and Service	70
8.4.	Responsibility and References	70
8.5.	Delivery	71

1. INTRODUCTION

The Trade Component of the USAID-funded Egyptian Technical Assistance for Policy Reform (TAPR-II) engagement requires an assessment of the Customs security and IT infrastructure components as a precursor to developing other aspects of the Egyptian Customs computing environment. This document provides supporting analysis and prescribed recommendations for implementation as part of the Egyptian Customs computing environment both during and beyond the Interim Modernization Phase in order to achieve a strategic end-state for Customs administration functions with an emphasis on security and IT infrastructure component needs. The recommendations set forth in this document prescribe the strategic end-state of the Customs security and IT infrastructure architecture and, where appropriate, further defines the recommended implementation order of architectural components to achieve this strategic end-state for the Customs security and supporting IT infrastructure of the Egyptian Customs computing environment.

1.1. Purpose

The purpose of this Customs Strategic IT Security-Infrastructure Analysis and Recommendations document is to provide practical and actionable recommendations and steps for improving the Egyptian Customs computing environment and achieving the desired strategic end-state for the Customs security and IT infrastructure components. Executing the recommendations of this document is considered a necessary prerequisite to pursuing other strategic Customs IT projects, such as:

- ❑ Installing and configuring an upgraded or replacement Customs Information System (CIS) as is currently under consideration
- ❑ Establishing two (or possibly three) main Customs processing sites that serve the other Customs sites with centralized CIS processing, data governance, etc. and provide for high availability, failover, and disaster recovery of the overall Egyptian Customs functions
- ❑ Upgrading any or all of the secondary (not main) Customs sites' security or IT infrastructure components in a consistent and interoperable manner with the main Customs sites and the other secondary sites
- ❑ Establishing overall Egyptian Customs IT Governance standards, processes, and methods and procedures (M & P's) in order to guide the future evolution of the Egyptian Customs computing environment in a strategic, predictable, and planned manner

Since some sites already have upgrade projects underway, and most are acting independently of such a strategic plan as recommended here, this highlights the sense of urgency for which these recommendations should be instituted across the Egyptian Customs enterprise architecture in order to promote planned consistency and completeness in its security and IT infrastructure components. Also, these recommendations will develop a foundation in order to support and coordinate all related Customs IT projects by first establishing and then maintaining the enterprise's security and IT infrastructure components over time.

1.2. Objectives

The key objectives of this document are to identify the key security and IT infrastructure components that are required within and across the Egyptian Customs organizations in order to achieve the prescribed strategic end-state, as well as to establish an order of events for building towards this end-state. Because of the broad reaching impacts of these objectives, the recommendations given here should further be prioritized and assigned in a follow-on management effort for how and when these will be addressed by the appropriate Egyptian

Customs stakeholders as identified in section 1.3 below. Note that this stakeholders list for those organizations directly or indirectly involved in Egyptian Customs processing is considered a place to start, such that this initial list will need to be refined as new stakeholders are discovered or established. For example, there is likely a future need for an IT Governance Board, IT Project Management Organization (PMO), CIS systems support group, centralized database support, etc.

While the objectives of this document include the identification of key security and IT infrastructure recommendations and the desired end-state (i.e. beyond the Interim Modernization Phase), two additional related objectives are to: 1) address the long-term issues in adjacent IT areas (e.g. enterprise architecture, workflow, systems, IT tools, skills, etc.) to the extent possible within the scope of this analysis; and 2) address the order of security and IT infrastructure component roll-out in order to facilitate coordination with Interim Modernization Phase efforts.

This document may also be adopted to serve as an agreement between TAPR-II and the Egyptian Customs Authority (ECA) regarding the security and IT infrastructure capabilities and requirements for the strategic end-state of the Egyptian Customs computing environment. Thus, an additional objective is that this document will provide a blueprint for strategic IT projects that will effectively coordinate and unify the overall enterprise architecture across Customs sites, especially in the areas of security and IT infrastructure. As such, this document or parts of it may potentially be provided to potential suppliers in order for them to prepare proposals to fulfill the recommended security and IT infrastructure components.

This is a living document—meaning that it will likely change over time, however much this is considered a solid “stake in the ground” at this time. Additional security needs and IT infrastructure requirements will be identified during the Customs reform process, and these changes should be reflected in future revisions of this document as well as in the subsequent IT planning and projects that will be initiated in order to achieve the strategic end-state recommendations. While the analysis and recommendations set forth herein are considered to be well-developed and thoroughly reviewed, there still must be a mechanism for reviewing and updating this document when appropriate changes are identified. It is recommended that this document be put under the guidance of an IT Governance Board or PMO for strategic execution of the recommendations and prudent control and evolution of the document and its content as needed.

1.2.1. Goals

In summary, the goals of this Customs Strategic IT Security-Infrastructure Analysis and Recommendations document are to:

- a) Identify the overall security (IT and non-IT) architecture gaps between the current situation and the strategic end-state (beyond the Interim Modernization Phase) of the Egyptian Customs computing environment
- b) Identify the overall IT infrastructure gaps between the current situation and the strategic end-state (beyond the Interim Modernization Phase) of the Egyptian Customs computing environment
- c) Where possible, further describe the prescribed order for implementation of the recommended strategic end-state architectural components as needed to progressively accomplish the overall strategic end-state of the Egyptian Customs computing environment

- d) Support the Interim Modernization Phase goals by prioritizing the security and IT infrastructure components clearly such that selected components may be included within Interim Modernization Phase planning and execution
- e) Document the risks associated with the identified security and IT infrastructure gaps
- f) Recommend potential solutions as potential IT-based and non-IT product and vendor examples, which can resolve and/or mitigate the risks of the identified gaps

While other advisors have worked extensively with Egyptian Customs recently, it is the intent of this analysis not to repeat the work previously performed, but instead to build upon and extend earlier analyses of the Egyptian Customs computing environment where appropriate to support the goals listed above. A primary intent here is to identify high priority and critical security and IT infrastructure gaps that need to be resolved as immediate activities in order to support the Interim Modernization Phase. Such high priority gaps may be addressed by Egyptian Customs, USAID, the European Union, and other contributing organizations as appropriate.

This analysis should be considered a benchmark of the current high-level security and IT infrastructure environment, while the recommendations for suggested solutions and priorities should be utilized as an initial high-level blueprint to be executed for moving forward and addressing the identified gaps and risks. This document takes a macro view of the Egyptian Customs computing environment, analyzing the overall situation across sites, while more and further detailed gap analyses for selected individual Customs sites may be prudent. Such selected follow-on analysis could influence this benchmark, as well as certain recommendations and priorities at each site, and would be applied to shape future versions of this document and the related tactical and strategic planning to upgrade the strategic end-state Egyptian Customs enterprise architecture.

1.2.2. Relationship with Interim Modernization Phase Goals

As these recommendations will lead to a strategic end-state of Egyptian Customs processing beyond that of the Interim Modernization Phase in the long term, particularly in the areas of security and IT infrastructure, they must also support and be coordinated with the goals of the Interim Modernization Phase in the short term. Hence, the highly prioritized steps towards the strategic end-state recommended here should be considered for inclusion in plans to achieve the Interim Modernization Phase state of the Egyptian Customs computing environment.

To summarize, the key goals of the Interim Modernization Phase are to:

- 1) Standardize all sites onto the latest version of the current Customs Commission Automated System (CCAS).
- 2) Create centralized data processing centers in Cairo (primary) and Alexandria (secondary), thus eliminating the need for separate databases at all operational locations.
- 3) Upgrade networks as necessary to support this centralized data processing.
- 4) Create a central database to support this centralized data processing, including an enterprise-wide data model for processing and reporting.
- 5) Address critical security (IT-based and non-IT) threats.
- 6) Improve management reporting.

Of these goals, recommendations from this Analysis will contribute directly to goals 2 through 6, and indirectly to goal 1. It will not contribute to the Interim Modernization Phase goal of standardizing onto the latest CCAS, as this is not considered a strategic long-term goal for the desired end-state of the Egyptian Customs computing environment.

1.3. Stakeholders

This document has been prepared primarily for Egyptian Customs, though it will also be generally useful for the donor community, including USAID and the European Union. Moreover, there are numerous stakeholders that will benefit from improving the security and IT infrastructure of the Egyptian Customs computing environment to achieve the prescribed strategic end-state. Primary stakeholders will include:

- ❑ Egyptian Customs Authority (ECA)
- ❑ General Office for Export and Import Control (GOEIC)
- ❑ Ministry of Finance (MoF)
- ❑ Traders/Importers/Exporters
- ❑ Freight Forwarders/Brokers
- ❑ Manufacturers
- ❑ Port Authorities (both Public and Private)
- ❑ General Authority for Free Zones and Investment (GAFI)
- ❑ General Deposit / Warehouses
- ❑ Ministry of Trade and Industry
- ❑ Ministry of Economy
- ❑ Ministry of Health
- ❑ Ministry of Agriculture
- ❑ Ministry of Foreign Affairs
- ❑ Chambers of Commerce
- ❑ International Transport Union
- ❑ Foreign Customs Administrations

More specifically within the ECA, GOEIC, and Port Authority stakeholders, the organizations and security and IT professionals that will be directly responsible for the implementation and maintenance of these security and infrastructure recommendations include the following “implementation stakeholders” (at and/or across all Customs sites):

- ❑ Customs Functional Requirements Analysts
- ❑ Customs Security (both IT and non-IT) and IT Management
- ❑ IT Department Management
- ❑ Security and IT Procurement Specialists
- ❑ IT Project Management
- ❑ Enterprise Architecture and IT Planning Specialists
- ❑ Systems Architecture and Integration Specialists (i.e. including the current Customs Commission Automated System and the future Customs Information System)
- ❑ Database Management and Data Warehouse Specialists
- ❑ Portal and Web Services Specialists
- ❑ Network Architecture and Planning Specialists
- ❑ Customs Security (both IT and non-IT) Specialists
- ❑ Remote Access Security Specialists

Note that many of the roles above and related skilled staff identified here either do not exist yet or are not defined well in order to support the Egyptian Customs functions. Hence, the identification and assignment of these implementation stakeholders should be treated as a high priority recommendation for organizational improvement, because filling these roles is a prerequisite to effectively addressing most of the Customs security and IT infrastructure gaps and risks identified in this document.

1.4. Scope

This analysis covers the overall security and IT infrastructure needs of the Egyptian Customs computing environment, and focuses on the related gaps and recommendations that should be addressed to achieve the strategic end-state, which is beyond the Interim Modernization Phase. Related issues and risks to the anticipated implementation of the resulting strategic Customs security and IT infrastructure end-state are also covered to the extent possible.

This analysis does not represent a commitment by the TAPR-II project to address the gaps, risks, or recommendations identified herein. However, it is intended to describe these in sufficient detail in order to facilitate discussion amongst the appropriate stakeholders and donors in order to best address them and build the strategic end-state for the Egyptian Customs computing environment.

The recommended strategic security and IT infrastructure will provide the infrastructure required to support a modern Customs Authority that complies with international standards and best practices. Even though some of the capabilities and functionality introduced in this document may not be needed immediately, the scope of the solution prescribed is intended to address all capabilities that will be required to achieve the long-term objective for successful completion of the Egyptian Customs reform process. To the extent possible, the short-term versus long-term priorities for implementation are called out with an explanation of the necessary sequential steps that will achieve this objective.

The prescribed security and IT infrastructure will facilitate the secure processing of information and documents for Egyptian imports and exports, gather trade statistics, and will coordinate document workflow and data sharing with other government and trade partner entities.

1.5. Constraints, Assumptions, and Dependencies

Numerous constraints, assumptions and dependencies have been highlighted in the Egyptian Customs IT Gap Analysis prepared by TAPR-II earlier in 2006, and this document will not restate all of these. However, the main constraints, assumptions and dependencies that will impact the successful implementation of the recommended security and IT infrastructure components of this document include:

- 1) The Egyptian Customs Authority (ECA) needs to complete a significant amount of recruitment and training for the necessary security and IT staff in order to support the implementation and maintenance of the recommendations prescribed in this document.
- 2) There are key IT projects currently planned or underway that will need to be coordinated with the implementation of the recommendations of this document. The most critical are the current projects for –
 - a. Upgrading the local area networks (LANs) in the Customs sites,
 - b. Implementing a new centralized Customs Information System (CIS) and a supporting centralized Customs operational database,

- c. Establishing a centralized Customs data warehouse, and
 - d. Increasing the capacity of the Raya wide area network (WAN) to support the new centralized Customs IT architecture.
- 3) Procurements take a substantial amount of time, and procurement plans need to be developed and tracked to ensure that the necessary hardware and software is available in time for the prioritized implementation steps of the prescribed security and IT infrastructure components recommended in this document.

1.6. Approach

In developing the analysis and recommendations of this report, the following key contributing sources were consulted:

- Previous related reports, including –
 - Functional Requirements Specification (FRS) for the Customs Information System (CIS) (May 2006)
 - Egyptian Customs Interim Modernization Phase IT Gap Analysis (Feb. 2006)
 - General Organization for Export and Import Control (GOEIC) Terms of Reference (TOR) for the Design and Implementation of Core Components of the Automated Inspection System (AIS) under the Clearance Automation Project (CAP) (Draft)
 - Technical Feasibility Study for the Implementation of the Automated System for Customs Data (Feb. 2004)
- Stakeholder interviews, including management and staff of the ECA, MoF, Port Authorities, GOEIC, and the Customs sites
- Customs site visits and interviews – Including Alexandria, Cairo Airport, Misr Station, Sohka, and Suez
- Meetings with Raya Communications to discuss the security, management, and monitoring of the Multi-Protocol Layer Switching (MPLS) Customs Intranet network currently managed by Raya on behalf of the ECA
- Industry research – Including applicable Customs and IT sources (e.g. web sites, white papers, presentations, and industry reviews for comparative solutions and best practices)

1.7. Approval Process

The Customs Strategic Security and IT Infrastructure document must be approved by the ECA before any of related projects or a request for proposal for procuring or implementing the recommended components can be initiated, since this approved document or selected parts of it will become key components of such project plans or an RFP. Just as the ECA is creating a committee in order to review the Functional Requirements Specification (FRS) for the new Customs Information System, such a committee should be established (or reused) to review this document and provide agreed-upon recommendations to the Commissioner.

2. SECURITY AND IT INFRASTRUCTURE STRATEGIC END-STATE

This section introduces the strategic end-state architecture of the Egyptian Customs computing environment, which will be achieved upon implementing the recommendations of this document. It describes the strategic end-state components and all relevant Egyptian Customs enterprise architecture and workflow interactions, with a particular emphasis on the prescribed security and IT infrastructure components of the end-state. Where possible, the order for implementation, and whether certain components are optional, is also detailed. The intent is to ensure the appropriate implementation stakeholders understand the need and role for each component, and when these should be introduced at each site. This will later assist in developing project and staffing plans for the implementation activities.

2.1. Reference Architectures

Two key reference architectures were developed for the Egyptian Customs processing sites in order to address both types of sites that comprise the overall Egyptian Customs enterprise architecture and computing environments. The appropriate site architecture to be applied for implementing a given site depends upon whether it is a “main” or “secondary” customs processing site, defined as:

- ❑ **Main Customs Processing Sites** – These sites are the primary, larger sites, where most customs information processing occurs, including that on behalf of secondary sites. Main sites will host centralized, shared customs information processing, including all the functions and capabilities of the new centralized Customs Information System (CIS), operational database, and a data warehouse. There is expected to be two or three main Customs sites, which is confirmed to include the Alexandria site as well as a new site at the Ministry of Finance (MoF) in Cairo. A third main customs processing site is currently under consideration for Port Said, but is not confirmed at the time of this report.

Each main site will be a duplicate of the other main site(s). These sites will support the local main site as well as selected secondary sites for the vast majority of all customs processing functions, as well as other selected centralized functions (i.e. e-mail). In addition, each main site will have the capability to provide failover, disaster recovery, load balancing, and backup services for the other main site(s) as needed.

- ❑ **Secondary Customs Processing Sites** – These more numerous sites will generally be access points and consumers of the services provided by the main sites.

Reference architectures for the main and secondary customs processing sites are shown below in Figure 1 and Figure 2, respectively. The contents of these diagrams are detailed in subsequent sections to describe the information technology security and infrastructure components and their interoperability of the Egyptian Customs strategic end-state for each type of site. These diagrams are also referenced in later sections when assessing gaps, risks, and priorities that need to be addressed in order to achieve the strategic end-state.

2.2. Main Customs Sites Architecture Solution

The recommended solution for the architecture of the main customs sites is shown below in Figure 1. As previously mentioned, this architecture will apply to the customs sites at Alexandria, a new site at the Cairo MoF, and possibly at Port Said (under consideration, to be determined).

In describing the details of the Main Customs Sites Reference Architecture, we begin by explaining the architectural goals and an overview of the main customs sites solution. Following this, we continue with an explanation of the details for each zone / domain that comprises the main customs sites architecture as shown in Figure 1 below.

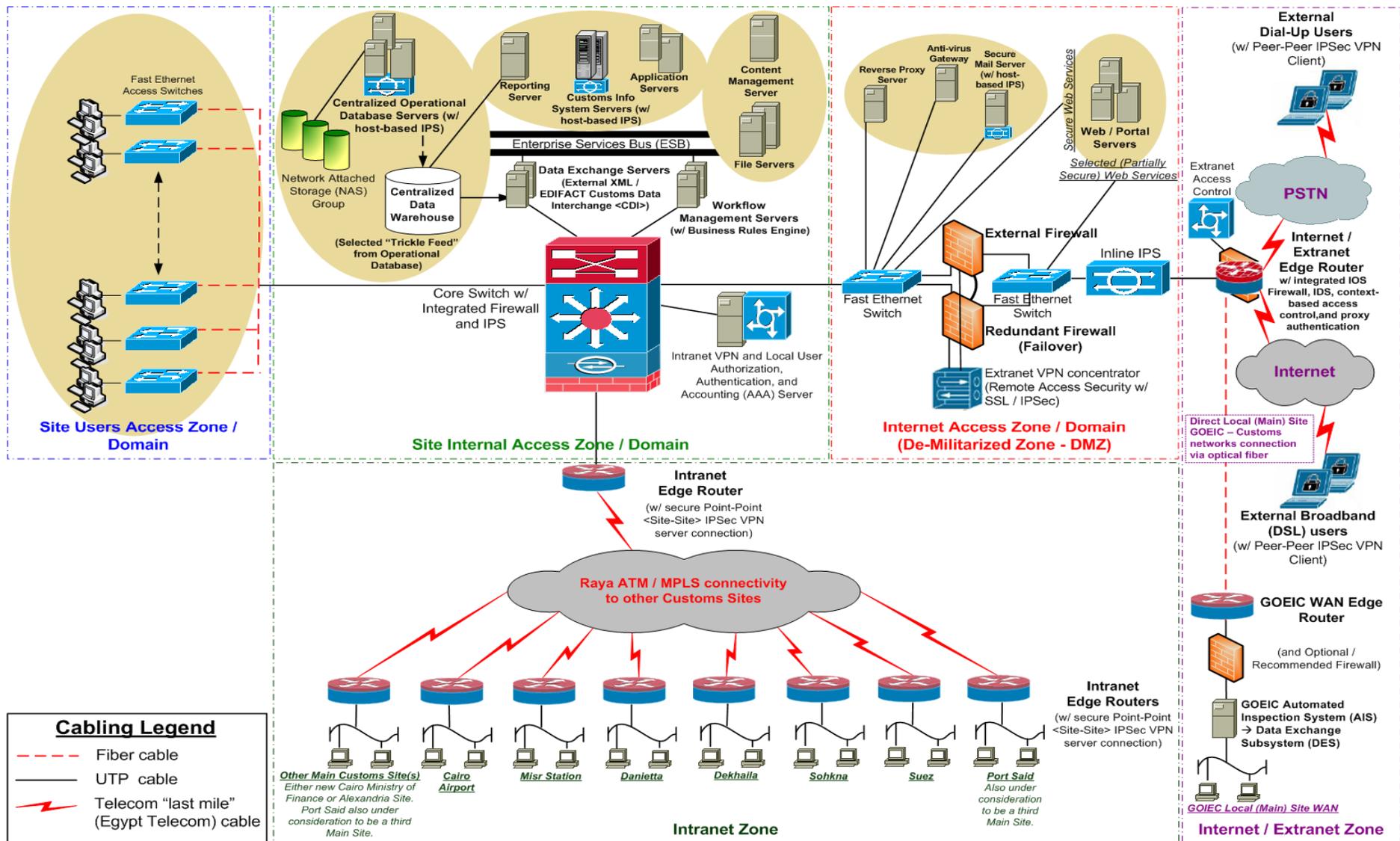


Figure 1. Main Customs Sites Reference Architecture

2.3. Main Customs Sites Architectural Goals

The primary architectural goals of the main customs processing sites are to:

- 1) Host the centralized, shared customs processing functions and components, including the Customs Information System (CIS), the Customs Operational Database (COD), the Customs Data Warehouse (CDW), customs management reporting, and the Customs Data Interchange (CDI) for external organizations' consumption of customs data.

- 2) Host centralized, shared services workflow capabilities.

Supporting the primary customs processing functions, the main sites will also host primary workflow management capabilities, including business rules, transaction queuing capabilities, and an enterprise services bus (ESB). Thus, a supporting architectural goal for hosting the centralized, shared customs processing functions is to facilitate a service-oriented architecture (SOA) that will underpin these functions and provide the workflow manageability, flexibility, robustness, and functional configurability needed to achieve this.

- 3) Provide an implementation migration path that will continue to support the current distributed customs processing at the secondary sites until the centralized, shared functions are ready to be hosted at the main site. Note that this architectural goal implies more current responsibilities for the secondary sites while customs processing and data sharing (i.e. with GOEIC) continues to be performed locally in advance of implementing the new CIS and centralized architecture at the main site. Nonetheless, this transition must be taken into account when planning and rolling out the new, improved main site architectural components and functions.
- 4) Host other non-customs (or indirect customs) processing centralized, shared services and components, including e-mail, Internet access, remote user access, intranet management, customs network and data security, and internal and external web and portal services.

These organizational IT infrastructure components will facilitate business within the main sites and between all (main and secondary) sites, ensuring the appropriate level of communications and security is maintained for all customs user groups.

- 5) Perform the primary customs and non-customs functional processing on behalf of all secondary customs sites.

For all the functions and components listed above, each main customs processing site will be responsible for selected secondary sites' processing (e.g. based on proximity and/or network load balancing between the sites) in order to ensure coverage for all secondary sites. The assignment of secondary sites to main sites may vary over time in order to facilitate main sites processing availability, maintenance, and upgrades as needed.

- 6) Provide failover, disaster recovery, load balancing, and backup services for all other main site(s) as needed.

These goals may be considered high level functional requirements for the main customs processing sites, such that a combination of these with the details outlined in subsequent sections may become a functional requirements basis for developing technical specifications as part of a request for proposal (RFP) and related vendor proposals for all or part of the overall solution.

2.4. Main Customs Sites Solution Overview

The main customs sites will achieve the goals listed above by applying an architecture that distributes the functional customs processing and access to the site's functions into

appropriate security zones. Each zone within the main site will be established as a local domain within the site's architecture, and each zone is delineated by a different "trust level" than its adjacent zones. Hence, there are security mechanisms that will be established at the perimeter between the zones with different trust levels in addition to the security mechanisms established within selected zones, in order to protect sensitive data or functions that would otherwise be at risk from unsecured transaction requests originating from a zone with a lower trust level.

Descriptions of the applicable security zones / domains for the main customs processing sites are (right to left, top to bottom in Figure 1):

- ❑ Internet / Extranet Zone – This zone includes user groups and transactions that must be treated as the highest risk for the main customs sites, because it generally contains public Internet and Public Switched Telephone Network (PSTN) traffic for which there is no control before it enters the zones of the customs site. In the case of valid users and transactions originating from the Internet zone, a secure and encrypted peer-to-peer virtual private network (VPN) Extranet will be first established between each user (peer-to-peer) and the main customs site. Also originating from the Internet / Extranet Zone is GOEIC access in order to acquire needed customs reference data for its back-end processing. In the case of GOEIC, access to the customs main site is via fiber optic cable and site-to-site encrypted VPN connection.
- ❑ Internet Access Zone (or De-Militarization Zone, DMZ) – This zone includes all components to directly handle transactions entering from the Internet / Extranet zone. It is the only access point from the Internet and PSTN, and is intended to only allow these types of security-controlled and filtered transactions:
 - 1) General public non-secure Web site access;
 - 2) Selected partially secure on-line web services for authorized users (not using VPN); and
 - 3) Fully secure VPN-enabled transactions for authorized users to enable back-end customs processing and communications through the secure VPN channel.
- ❑ Site Internal Access Zone – This zone hosts all of the centralized, shared back-end customs processing functions and components, including the Customs Information System (CIS), the Customs Operational Database (COD), the Customs Data Warehouse (CDW), customs management reporting, and the Customs Data Interchange (CDI) for external organizations' consumption of customs data. The only transaction requests that will be processed in this zone are those that have:
 - 1) Originated from the Extranet Zone and cleared all relevant security mechanisms (VPN encryption/decryption depending upon the request, one- or two-stage firewall depending on the request, and the inline Intrusion Protection System <IPS>);
 - 2) Originated from the local Site Users Access Zone (see below) and cleared the Authorization, Authentication, and Accounting (AAA) server; or
 - 3) Originated from the Customs Intranet Zone (see below) as well as cleared the Intranet security mechanisms (VPN, switch integrated firewall and IPS, and the AAA server).
- ❑ Site Users Access Zone – This zone contains all the local site user workstations. This could potentially mean all desktops, laptops, and handheld devices at the site, as well as Ethernet switches, hubs, and wireless local area network (WLAN) components, if any. However, for the purposes of this the proposed solution, and in

the interest of promoting a highly secure customs processing environment, this architecture only recommends desktop workstations connected by Ethernet switches. Allowing any of these other access device types has the potential to expose the otherwise secure customs network to unwanted requests. It is recommended to not allow these initially and only later on when further appropriate security mechanisms are put into place.

For example, it is anticipated that handheld device access via WLAN could be prudent for selected customs functions at a later date (e.g. to process radio frequency identification <RFID> tags at loading docks or in customs goods warehouses). In advance of instituting such access and functionality, an encrypted, secure WLAN would need to be established, and processes would need to be created and managed for the inventory, software, and location management of the limited number of allowed handheld devices. This would all occur within the Site Users Access Zone.

- ❑ Intranet Zone – This zone is strictly for the Egyptian Customs Intranet (ECI), which includes the Raya managed MPLS network as well as the Egypt Telecom “last mile” or connectivity that provides the primary data communications between all main and secondary customs sites. It is intended to only allow security-controlled and filtered transactions for authorized customs users to enable back-end customs processing and communications through a fully secure site-to-site VPN channel.

Each of these zones / domains is further detailed by its user groups and infrastructure components in separate subsequent sections below.

2.4.1. Main Internet / Extranet Zone User Groups and Infrastructure Components

The user groups of the Intranet / Extranet Zone are as follows:

- ❑ External dial-up customs end users – These customs users are authorized customs VPN users who access the customs site processes via a secure peer-to-peer dial-up connection over the PSTN. It should be noted that only main customs processing sites allow these types of RA users; as will be seen while detailing the secondary customs sites architecture, there is no remote user access.
- ❑ External broadband (DSL) customs end users – These customs users are authorized customs VPN users who access the customs site processes via a secure peer-to-peer broadband connection over the Internet. The broadband technology currently used for this broadband connectivity is Digital Subscriber Line (DSL) but could also (or instead) be Cable Modem in the future. It should be noted that only main customs processing sites allow these types of RA users; as will be seen while detailing the secondary customs sites architecture, there is no remote user access.
- ❑ GOEIC wide area network (WAN) – GOEIC access to the customs site is an authorized secure site-to-site VPN connection over a local site fiber optic cable for the purpose of acquiring selected customs reference data that will be regularly processed by the GOEIC Automated Inspection System (AIS). It should be noted that both main and secondary customs processing sites allow this type of GOEIC VPN access.

The infrastructure components and related processes of the Intranet / Extranet Zone are as follows:

- ❑ Remote Access (RA) workstations – These are the desktops and laptops of external customs users (both dial-up and broadband) and are generally located and managed at the authorized user’s remote office.

Remote access may also be from customs users' homes if allowable according to Egyptian Customs RA policies (to be determined), but because this may not be manageable it should be assumed that the workstation access point itself is not secure. However, authorized workstations must have access to the appropriate network modem (either PSTN dial-up or Internet DSL broadband) for basic network connectivity, as well as the appropriate matching VPN software for the network type.

- VPN software and RA security tokens – In order to facilitate secure VPN connections for RA user workstations and the GOEIC WAN, as well as to control the proliferation and manageability of this VPN access, the appropriate VPN software and security tokens will be used. The VPN software licenses and physical tokens will be inventory controlled and managed in order to ensure that it is always known who has access to customs site processing and data.

Secure tokens are used to increase the level of security and verify the authenticity of the holder. This will be used when the RA end user (or GOEIC server) is logging into the customs network. Such a secure token is a device that constantly displays a secure code that can be used to authenticate a user to the back-end trusted customs network source. This form of authentication is more secure than just password phrases, because it constantly changes the secret code. A secure token can take the form of a dongle, smart card, USB pen drive, cell phone, or any computing device that is portable and easily carried around with the user. For the purposes of this report, we are referring to one of the most common and portable of these options, the dongle, and this may either be external (e.g. a number is read by the user to be entered at a prompt) or a USB dongle to be inserted into the workstation / server. The other types, however, may be considered if desirable by the ECA. While these devices are presently expensive, prices are falling to make it affordable for low level personnel. Note that secure tokens, like local physical security access, will eventually be replaced by some form of biometric data validation.

The appropriate VPN software will establish a secure channel between the RA end user and the customs site. The two most popular VPN models are either using the Internet Protocol Security (IPSec) or Secure Socket Layer (SSL); however, while SSL VPNs are easier to manage, IPSec is widely considered more secure when used within both Internet and Multi-Protocol Label Switching (MPLS) networks, so for the purposes of this report, we concentrate only on a VPN implementation for Egyptian Customs utilizing IPSec. Also, IPSec essentially includes extensions to Internet Protocol v4 (IPv4), and these extensions will eventually be required for the implementation of IPv6 in the future.

While not a complete list, some examples of IPSec VPN vendor software that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, NetGear, SonicWALL, WatchGuard, Symantec, Enterasys, and FireBox. Note that the customs site VPN software and the RA user client VPN software (on the remote workstation) needs to be compatible, so it is recommended that these be from the same vendor. This will also ensure no support gaps in the overall VPN solution.

Similarly, some examples of secure physical tokens are listed here by vendor, which can be used for the selected VPN solution as an initial list for further investigation and analysis in filling this need are – RSA, Entrust, ID Control, Matrix, and Omnikey. A secure token can take the form of a smart card, ID, USB pen drive, or a dongle

- PSTN and Internet broadband connectivity – This is simply the network connectivity between the RA end user and the Internet / Extranet Edge Router at the main customs sites. It currently includes the Egypt Telecom PSTN for dial-up users, and either Raya or Nile-Online DSL Internet connectivity for broadband users. Also

assumed in the overall connectivity for broadband users to the customs site is the need for an Egypt Telecom “last mile” connection from the primary DSL network to the site’s Internet / Extranet Edge Router.

- ❑ Internet / Extranet Edge Router – This is the Ethernet Router at the perimeter of the customs site network for external access. It is the concentration point for all Internet / Extranet transactions from either external users or the GOEIC WAN, and is the only access point to the customs site Internet Access Zone or DMZ. This edge router should ideally include an integrated Internetwork Operating System (IOS) firewall, Intrusion Detection System (IDS), context-based access control, and proxy authentication. Otherwise, these supporting functions will need to be provided by an adjacent device or server (e.g. Extranet Access Control, see below).

While not a complete list, some examples of appropriate edge router vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, Juniper, Laurel, and Lucent.

- ❑ Extranet Access Control – This access control software may either be integrated into the Internet / Extranet Edge Router or provided on an adjacent device / server that is connected to the router. It provides the first line of defense for the Extranet VPN by controlling VPN user access authentication, as well as context-based access control and proxy authentication if any of these services are not integrated into the Internet / Extranet Edge Router.
- ❑ GOEIC-to-Customs site fiber cable connection – This is an optical fiber cable hardware connection between the GOEIC WAN Edge Router and the customs site Internet / Extranet Edge Router. In some sites, this connection already exists but may need to be secured by firewalls on both the customs network side and GOEIC network sides of the connection. In other sites, the fiber cable either needs to be laid or replaced to establish this connection (and then appropriately firewalled on both sides of the connection).
- ❑ GOEIC WAN and Edge Router – The GOEIC WAN encompasses all the local site systems and automated processes, including the Automated Inspection System (AIS). This system requires information from the Customs Information System (CIS) database and will receive this data via a secure VPN channel between the GOEIC WAN Edge Router and the customs site Internet / Extranet Edge Router (over the fiber cable physical connection). Within the GOEIC WAN, the Data Exchange Subsystem (DES) of the AIS will translate the XML data acquired from the CIS database.

Also, there should be a firewall established at the edge router to protect the AIS and DES from unwanted attacks UNLESS this router only services the fiber connection between GOEIC and the customs site (i.e. the router has no other connection). For the purposes of this report, it is assumed that the GOEIC WAN Edge Router services other external transaction requests and should be treated as an internet / extranet edge router with the appropriate firewall (and furthermore anti-virus and IPS) protections. It is generally beyond the scope of this report to provide recommendations to GOEIC for its WAN, but it is also in the best interest of Egyptian Customs for GOEIC to provide a fully secure network when connected with customs sites.

2.4.2. Main Internet Access Zone (DMZ) User Groups and Infrastructure Components

The user groups of the Internet Access Zone are as follows:

- ❑ Remote access (RA) end users – These are the external dial-up and broadband customs end users as defined above for the Internet / Extranet Zone. In the case of the Internet Access Zone, the transaction requests from these end users will have already been validated and filtered by the Internet / Extranet Edge Router, firewall, and external access control components of the Internet / Extranet Zone prior to entering this more secure zone.

Transaction requests from this user group may either be processed within the Internet Access Zone, as in the case of partially or fully secure web services or e-mail services, or within the adjacent Site Internal Access Zone, as in the case of CIS processing or to gather data from the CIS database or data warehouse. Since these latter components reside within the Site Internal Access Zone, it is intended that valid CIS transaction requests from these end users will traverse past the Internet Access Zone to be processed in this more secure zone. The routing of end user transactions to the Site Internal Access Zone components will be assisted by the Internet Access Zone's reverse proxy server to determine which destination server is appropriate to field each transaction.

- ❑ GOEIC wide area network (WAN) – As is for the RA end users, GOEIC data transaction requests will have already been validated and filtered by the Internet / Extranet Edge Router, firewall, and external access control of the Internet / Extranet Zone prior to entering this more secure zone.

Since GOEIC transactions are intended to gather reference data from the CIS database and data warehouse, and these components reside within the Site Internal Access Zone, it is intended that valid GOEIC transaction requests will traverse past the Internet Access Zone to be processed in this more secure zone. Also, as is with end user transactions, the routing of GOEIC transactions to the Site Internal Access Zone components may be assisted by the Internet Access Zone's reverse proxy server to determine which destination server is appropriate to field each transaction.

However, at a later time when the site's components and servers, as well as the GOEIC processes, have matured and stabilized such that it is readily understood with a small number of types of GOEIC transactions that are always processed in the same server(s), then the reverse proxy server may be bypassed for GOEIC transactions.

- ❑ Site Users – Local site users will also use the CIS functions and data of the Site Internal Access Zone, as well as the e-mail and secure web services of the Internet Access Zone. However, since transaction requests from site users will originate from the more secure Site Users Access Zone (far left of Figure 1), there are generally no additional security mechanisms required other than the local anti-virus, IPS, firewall, and VPN functions as located within each of these other zones.

For example, in order to utilize the secure mail server that resides within the Internet Access Zone, the Anti-virus gateway, host-based mail server IPS, external firewall, and VPN encryption are applied within that zone. Similarly, all these local Internet Access Zone security mechanisms, minus a host-based IPS, are applied for accessing the secure web services. Of course, the reverse proxy server is not used for internal user requests, as these are originating behind the firewalls and DMZ.

The infrastructure components and related processes of the Internet Access Zone are as follows (right to left and bottom to top in Figure 1):

- ❑ Inline Intrusion Protection System (IPS) – This is the first line of defense against all external attacks (e.g. viruses, worms, denial-of-service <DoS>, etc.) and other unwanted accesses (e.g. invalid usage) within the Internet Access Zone. Thus, at this point, requests have cleared the edge router, as well as the firewall, IDS, and

Extranet Access Control components of the Internet / Extranet Zone. It is now the responsibility of the inline IPS to review all incoming transactions, through deep packet inspection in search of such unwanted usage, and provide alerts or shut down access as deemed appropriate.

Egyptian Customs must monitor their networks for unauthorized intrusions, as hackers will be interested in crashing systems, deleting and / or manipulating data, and stealing data. Due to the sophistication of hackers, Customs needs to go beyond properly configuring servers and implementing firewalls. Instead, network intrusion software is another important tool for preventing unauthorized access to the Customs networks and systems by monitoring networks and identifying suspicious and malicious activity. Customs needs to acquire and implement network intrusion software as soon as possible and have key IT staff trained on how to use it properly.

An inline or Network-based IPS (NIPS) has the capability to provide security at all system levels from the operating system kernel to network data packets. It provides policies and rules for network traffic for alerting the system or network administrators to suspicious traffic, and allows the administrator to prescribe in advance any appropriate actions for the NIPS to take upon being alerted. Where traditional Intrusion Detection Systems (IDS) would inform about a potential attack, an IPS makes attempts to stop it. Another significant leap over IDS capabilities is that the IPS has the capability of being able to prevent known intrusion signatures, but also some unknown attacks due to its database of generic attack behaviors.

A highly functioning stateful IPS will correctly identify patterns of transactions and embedded data via dynamic rule updates in order to determine the nature of usages to either allow or disallow their downstream processing. Hence, only transaction requests that are allowed by the IPS will be further processed by the web / portal servers, external firewall, VPN concentrator, reverse proxy server, or secure mail server of the Internet Access Zone, or by components of the Site Internal Access Zone (e.g. the CIS, database, data warehouse, etc.).

While not a complete list, some examples of appropriate inline IPS vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, Network Associates, Sana Security, ForeScout Technologies, StoneGate, TippingPoint, Enterasys, and IntruPro.

- Fast Ethernet Switches – These are generally 100 Megabit per second (100-Mbps or 100BaseT) Ethernet switches intended for fast local area network (LAN) traffic routing. In the case of the Egyptian Customs network, 100BaseT4 switches are required for four pairs of (voice or) data-grade Category 5 wiring. Note that Gigabit switches (1,000 Mbps) may also be considered, but at this time these are considered “overkill” for the anticipated Egyptian Customs processing needs. However, particularly at main customs processing sites, a case can be made for needing this additional bandwidth for future growth as centralized services become more prevalent here on behalf of all secondary sites (and GOEIC instances).

While not a complete list, some examples of appropriate fast Ethernet switch vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, NetGear, D-Link, 3Com, and TrendWare.

- External and Redundant Firewalls – These are combination Open Systems Interconnect (OSI) Layers 3 (Network), 4 (Transport), and 7 (Application) firewalls intended enforce policies for transactions that involve secure services both within the Internet Access Zone (i.e. secure mail or web services) or within the Site Internal Access Zone (i.e. CIS services).

A word about choosing the right firewall:

Traditional firewalls operate at Layers 3 and 4 of the OSI model. Layer 3 firewalls, operating at the Network Layer, perform simple packet filtering, examining each packet passing through and making a decision about whether to forward or drop the packet. For example, a firewall that only allows outgoing Web traffic would contain a rule that allows packets with destination port 80 from any internal IP address to any IP address on the Internet. To allow the return packets from Internet-based web servers a second rule is required: Allow packets with source port 80 from any IP address on the Internet to any internal IP address. It didn't take hackers long to figure out that such rules allow them to send any traffic they choose into someone's internal network as long as the attack tools use port 80 as the source port. Thus, no serious firewall today relies on packet filtering alone.

Stateful inspection was developed to address the limitations of packet filtering. This type of protection operates at Layer 4, the Transport Layer. Stateful firewalls examine entire connections between computers, instead of just single IP packets. In the example of outgoing Internet traffic, a stateful firewall allows incoming packets from port 80 on an external computer only if they belong to a connection that was initiated to that port from an internal computer. Other incoming packets are dropped, even if their TCP source port is 80. In addition, stateful inspection also tries to ensure the integrity of the connection itself, guarding against attacks such as TCP session hijacking, which is an attempt to take control of an existing, legitimate connection.

The problem with relying on packet filtering and stateful inspection alone is that most attacks today use legitimate ports and allowed connections. If you're not providing access to a web server, you can easily protect your network by configuring your firewall to drop all traffic addressed to port 80 on your computers. However, if you have a public web server as we intend to for Egyptian Customs, we will have to allow inbound traffic to the server on port 80. Packet filtering and stateful inspection will allow all such traffic to reach the server. Hackers know this and most of today's attacks use allowed connections and aren't based on bypassing packet filters or playing tricks with TCP connections. Instead, they attack applications such as a web server, mail server, or a client program like a browser over valid connections and allowed ports.

Thus, a firewall that also addresses Layer 7 (Application Layer) is needed for sufficient protection of the Customs networks. Application-layer filtering is crucial to protect today's networks. Of all firewall criteria, application-layer protection is the most important feature today. For the Customs computing environment, this should be a primary item evaluated. Application-layer capabilities are what most differentiate firewall vendors today, and finding the right firewall can be a complicated task. Also, some Layer 7 firewalls suffer a performance hit because their firewalls weren't originally designed to do Layer 7 filtering.

While not a complete list, some examples of appropriate firewall vendors that can be used as an initial list for further investigation and analysis in filling this need are – Microsoft, Checkpoint, Cisco, Clavister, CheckPoint, and WatchGuard. Initial analysis has uncovered that –

- Two of the most advanced application-layer firewalls are CheckPoint's FireWall-1 and Microsoft's ISA Server

- Cisco's PIX firewall, the most popular hardware firewall, is very good at packet filtering; however, if you add application-layer filtering capabilities via add-ons, there may be performance degradation
- WatchGuard Technologies has recently added new features to its line of firewalls and provides some of the best application-layer protection amongst hardware firewalls.

Note that the redundant firewall can further secure the customs environment by providing primary firewall failover or load balancing capabilities as well as by introducing an alternative firewall technology (i.e. if it is of equal functionality but acquired from a different vendor with presumably different weaknesses). Hence, it is useful to acquire one each of the top two firewalls deemed appropriate for the DMZ to be the primary and redundant firewalls.

- Extranet VPN Concentrator – This device or software is responsible for the incoming / outgoing decryption / encryption services as well as concentrating all VPN-related traffic at the external firewall. The choice of VPN concentrator software must, of course, be compatible with the client VPN software used by external users and GOEIC.

A word about choosing VPN vs. Citrix technologies:

The primary traditional VPN technologies are SSL or IPSec and, as discussed earlier we are focusing on IPSec as the more secure VPN technology. Note, however, that an alternative technology to traditional VPNs that should be considered is Citrix in regards to its thin client offerings (Metaframe Presentation Server). The technologies and components employed for a Citrix solution differ tremendously from a traditional VPN. The main differences are that a VPN concentrator is an appliance that will allow you to manage a number of IPSec and / or SSL connections but will not provide you with thin client access to applications that are not otherwise present on the user's laptop / device. Citrix Metaframe will, however, allow you to grant access to applications on the Customs network that are not necessarily installed locally on the user's laptop / device. If Customs were to utilize Citrix Metaframe, there may be benefits over a VPN solution if it is intended that remote users would need to use the new CIS (or some other back-end applications) directly. This is to be determined, and should be re-evaluated while and after the new CIS vendor is chosen. However, be warned that a Citrix installation generally implies much higher installation costs. For the reasons of an undetermined need for direct back-end application access and much higher installation costs, a VPN solution is likely the best choice for the Egyptian Customs networks.

Note some of the main features that the Citrix Access Gateway has over a traditional (e.g. Cisco) VPN concentrator are:

- URL Distributed Client
- Centralized Client Management and updates
- Concurrent Licensing model
- SSL Tunnel (i.e. as apposed to Cisco best route technology)
- Application access control
- Split Tunneling On / Off (i.e. stops worm transversal)
- Client Checking (Checksum checks)

However, because of the reasons listed previously, for the purposes of this report we concentrate on an IPSec VPN solution for the Egyptian Customs

computing environment.

While not a complete list, some examples of appropriate VPN concentrator vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, VPNet, CheckPoint, TimeStep, Xedia, Technologic, Nortel, Compatible Systems, Lucent, and Assured Digital.

- Web / Portal Servers – These may be standard web servers (i.e. computers on the World Wide Web that store HTML documents which can be retrieved via a web browser), portal servers that work with a particular back-end platform (i.e. Microsoft, Oracle, etc.), or a combination of these for selected web services. It is recommended that a standard web server platform be adopted for all Customs non- or partially-secure web services. These will be for services provided through the Customs website and not requiring encryption or strong authentication.

For secure, encrypted web services, these may be provided via the same web server platform and / or via portal servers that augment the back-end platform and processes. For example, if Oracle is adopted as the strategic database and data warehouse platform for Customs data and the new CIS, then it will be more efficient to deploy Oracle Portal Services for access to selected data. Similarly, if Microsoft SQL Server is adopted as the strategic data platform, then MS SharePoint Portal and SharePoint Services will be a logical choice for selected portal services. However, since the choice of CIS vendor and related platform decisions are yet to be made, and there is a definite immediate need for Customs web servers, for the purposes of this report we concentrate on filling this need.

While not a complete list, some examples of appropriate web server vendors that can be used as an initial list for further investigation and analysis in filling this need are – Microsoft (IIS), Apache, Covalent, Roxen, Servotec, Xitami, and LightSpeed.

The two most prevalent web servers in the industry are Microsoft IIS and the Apache Web Server. These are compared and contrasted below in Table 1:

	<u>Microsoft Internet Information Services</u>	<u>Apache Web Server</u>
Latest Version	6.0	2.2.0
Price Details	Included with all Windows Server 2003 versions	Free
Vendor	Microsoft	Apache Software Foundation
Description	Web server that works in conjunction with Windows Server operating systems	The predominant open source Web server
Administration Features:		
GUI Configuration	✓	✓
GUI Setup	✓	✓
Remote Administration	✓	✓
SNMP Configurable /	✓	✓

Monitorable		
Flexibility / Scalability Features:		
.NET compliant		
64-bit port		
Cluster Support		
IPv6 Support		
J2EE 1.4 compliant		
Multiple Logs		
Supports Microsoft ISAPI		
Virtual Servers		
Web-based Interface		
Programming / Scripting Features		
Includes Source		
Own API		
Own Scripting / Batch Language		
Supports External Scripting / Batch Language		
Security Features		
Active Directory Authentication		
Anti-virus capabilities		
Built-in firewall		
Built-in proxy capabilities		
Internal user access scheme		
LDAP Authentication		
Other / System Authentication		
SSL (Hardware)		
SSL (Software)		

Support Features		
Commercial Support Available	✓	✓
Forum Support	✓	✓
Mailing List Support		✓
Service Level Agreement Offerings Available	✓	✓

Table 1. Industry Leading Web Servers Comparison

- Secure Mail Server (with host-based IPS) – In the case of secure mail servers, the logical choice (and dominant player in the industry) is Microsoft Exchange Server 2003. However, if we wish to compare and contrast other competitive mail servers, the following should be considered – IBM Lotus Domino, Kerio MailServer, OpenXchange Server, and Scalix.

Also, because the mail server has highly sensitive data and its availability is considered critical for Customs operations, it will be specifically protected from unwanted access or malicious attacks by a host-based IPS (HIPS), in addition to those threats that would otherwise have been alleviated by the upstream inline IPS and external firewall. A HIPS works much like the inline NIPS described earlier, but it is tuned and focused especially for the types of threats posed to mail servers; thus it is more effective in removing such specific e-mail threats.

HIPS are used to protect servers through software that runs between your system's applications and the OS kernel. The software is preconfigured to determine the protection rules based on intrusion and attack signatures. The HIPS will catch suspicious activity on the system and then, depending on the predefined rules, it will either block or allow the event to happen. HIPS monitors activities such as application or data requests, network connection attempts, and read or write attempts, etc.

While not a complete list, some examples of appropriate host-based IPS (HIPS) vendors that can be used as an initial list for further investigation and analysis in filling this need are – McAfee, Cisco, Sana, and Symantec.

- Anti-Virus Gateway – Such an enterprise-level anti-virus gateway will provide high-performance, comprehensive, multi-layered protection against viruses, spam, and unwanted email and web content at the Internet gateway. A highly functioning anti-virus gateway will provide the following features:
 - Offers multi-layered spam prevention by combining blacklists and heuristic detection with whitelists in order to maximize detection and minimize false positives
 - Provides secure remote management, advanced outbreak alerting, and concise reporting to view key performance and scanning metrics and overall system status
 - Enables transparent virus definition and scan engine updates without restarting services or reinstalling software
 - Delivers scalable, high-performance scanning with minimal network impact

- Includes scheduled delivery of antivirus and URL filter list updates, ensuring up-to-date protection

While not a complete list, some examples of appropriate anti-virus gateway vendors that can be used as an initial list for further investigation and analysis in filling this need are – Symantec, Trend Micro, Sybari, McAfee, Microworld, GFI, Finjan, F-Secure, Esset, Computer Associates, and Sophos.

- Reverse Proxy Server – This may be a separate proxy server, or may be a feature included with the external firewall software, as is becoming a trend amongst vendors. Thus, an advantageous choice of an external firewall that also has reverse proxy capabilities will reduce the need for a separate server / device for this purpose.

In its simplest form, a reverse proxy server is a layer that sits between a local area network (LAN) and an external network such as the Internet. The proxy server serves several needs, including –

1. Enable several servers to share a single Internet connection by accepting and forwarding requests from the client (end user and GOEIC) applications
2. Regulate (allowing or disallowing) certain communications with the outside world through site filtering
3. Conserve bandwidth and increase network efficiency by caching content for repeated local delivery

Thus, the reverse proxy server shares Internet access at the application level, which means that every client program must be individually configured to talk to the proxy server. This is an effective way to allow limited kinds of Internet access, though it should be noted that the configuration requirements can become a burden.

As mentioned above, the reverse proxy server as a stand-alone product is becoming an endangered species, and it is more likely that we will solve this need in coordination with the selection of appropriate firewall servers. However, in the case that we need to seek reverse proxy specialist devices / software, here are some examples of reverse proxy server vendors that would be appropriate and can be used as an initial list for further investigation and analysis in filling this need are – Netegrity, Microsoft, Sun, and Squid.

2.4.3. Main Site Internal Access Zone User Groups and Infrastructure Components

The user groups of the Main Site Internal Access Zone are as follows:

- Remote access (RA) end users – These are the same external dial-up and broadband customs end users as defined above. In the case of the Internal Access Zone, the transaction requests from these end users will have already been validated and filtered by the Internet / Extranet Edge Router and external access control, two-stages of firewalls, and the inline network IPS (NIPS) prior to entering this most secure Customs processing zone. Transaction requests from this user group that will be processed within the Site Internal Access Zone are those such as in the case of CIS processing or to gather data from the CIS database or data warehouse.
- GOEIC wide area network (WAN) – As is for the RA end users, the GOEIC data transaction requests will have already been sufficiently validated and filtered by the security mechanisms of the Internet / Extranet and Internet Access (DMZ) zones

prior to entering this most secure Customs processing zone. GOEIC transactions are intended to gather customs reference data from the CIS database and data warehouse, which all reside within the Site Internal Access Zone.

- Site Users – Local site users will also use the CIS functions and data of the Site Internal Access Zone. Also, since transaction requests from site users will originate from the secure Site Users Access Zone (far left of Figure 1), there are generally no additional security mechanisms required other than the local anti-virus and IPS functions located on selected servers within this zone.
- Customs Intranet Users – Customs processing users located at other customs sites will access the CIS functions and data via the Intranet Edge Router that connects the main customs processing site to all other (main and secondary) sites. The processes for which the other sites would use at this main customs processing site depend upon whether the requesting site is another main site or a secondary site, as follows –
 - Other main sites will coordinate with this main site for Customs data synchronization, backup, failover, and load balancing. These sites are essentially duplicates, and the challenge is to keep them as such while each one is processing for a limited number of secondary sites.
 - Secondary sites will use the main site for their primary Customs processing via the CIS, as well as access to the Customs data in the operational database and data warehouse.

The infrastructure components and related processes of the Internal Access Zone are as follows (right to left and bottom to top in Figure 1):

- Intranet VPN and Local User Authorization, Authentication, and Accounting (AAA) Server – This is typical AAA server software to handle user requests for access to (Customs internal) computer resources and to provide authentication, authorization, and accounting services for the Customs enterprise. In this case, the AAA services are to facilitate the authorization and authentication of valid local users and valid remote Intranet users of the CIS processes and data.

While not a complete list, some examples of appropriate AAA server vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, Hewlett-Packard, ActiveIdentity, Telecount, and Merit.

- Core Switch with Integrated Firewall and IPS – This core switch is intended to do the “heavy lifting” of the switching between all the various servers that reside within the Internal Access Zone on behalf of local site users, Customs Intranet users, Customs Extranet end users, and GOEIC usage. On behalf of the local end users and remote Customs Extranet end users, this switch provides the appropriate switching between the relevant servers for Customs workflow and data access. However, for Intranet user requests that are originating from the less secure Intranet Zone, the core switch’s integrated firewall and IPS services are utilized for additional security before switching the request within the Internal Access Zone.

While not a complete list, some examples of appropriate core switch vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, PMC-Sierra, Extreme Networks, Enterasys, Force10 Networks, and Foundry Networks.

- Workflow Management Servers – These servers will control the workflow for all customs back-end processing, including the automated steps and business rules for regular and dynamic customs processes and data inputs and outputs. Thus, the workflow management servers will directly control the operations of the new CIS and

data exchange servers, as well as their supporting operational database management and data warehouse solutions.

While not a complete list, some examples of appropriate workflow management server vendors that can be used as an initial list for further investigation and analysis in filling this need are – Microsoft (BizTalk, BizTalk Business Rules Engine, and MSMQ Server), IBM (WebSphere, WebSphere BusinessBeans, and JRules), Oracle, and Tibco (BusinessWorks).

- Enterprise Services Bus (ESB) – The ESB is an extension of the workflow management servers, and generally enables the services for workflow management across a broad spectrum of applications and services by enabling connectivity to these centralized workflow and business rules capabilities via standard and customized application and server adapters for the workflow management servers.

The ESB is an essential component in the implementation of a service-oriented architecture (SOA) as is necessary in such a centralized workflow and business rules processing intensive environment such as for Egyptian Customs. Also, since the ESB is an extension of the selected workflow management solution, the same list of example vendors applies, though in the case of non-Microsoft workflow management there is the ability to mix and match vendors to some extent.

- Data Exchange Servers (or the Customs Data Interchange <CDI>) – These servers will make selected customs data from the operational database and/or data warehouse available to external data consumers. Initially, this is expected to be used primarily to service the GOEIC need for regular, near real-time customs reference data in XML format. In the future, the Data Exchange Servers may provide data to additional consumers such as banks in other data exchange formats such as EDIFACT.

While not a complete list, some examples of appropriate data exchange server vendors that can be used as an initial list for further investigation and analysis in filling this need are – Microsoft (BizTalk and MSMQ), IBM (WebSphere and WebSphere MQ), Oracle, and Tibco (BusinessConnect). However, if a strategic decision is made for the Customs database platform to be Microsoft SQL Server, then this strengthens the case for Microsoft components in the Data Exchange Server capacity. If Oracle is chosen for the database platform, however, any of the other vendors can provide a compatible data exchange server.

- Content Management Server and File Servers – These servers will fill the Main site needs for shared: 1) web page and document content management for the Egyptian Customs website and web services, 2) customs back-end document and image processing, and 3) basic file management for all local and supported secondary customs sites users.

While not a complete list, some examples of appropriate content and file management server vendors that can be used as an initial list for further investigation and analysis in filling these needs are – Microsoft, FileNet, Oracle, Interwoven, and Accumo. Also note that some of these vendors have particular strengths that make it possibly desirable to employ more than one Content Management solution (e.g. FileNet is particularly strong for document and image processing, while Microsoft Content Manager is stronger for web content management).

- Customs Information System (CIS) Servers with host-based IPS – This will be the new Customs system replacement for the current Customs Commission Automated System (CCAS), for which the functional requirements have been completed and a vendor will be chosen in the near future. The supporting application servers and

database management servers will depend upon the selected vendor and its product installation and configuration requirements.

In terms of its application servers, it is assumed for the purposes of this report that these will either be for a Java open source platform or a Microsoft-based platform. Hence, while not a complete list of the many available application server vendors, some example vendors that may be used as an initial list for further investigation and analysis are – Microsoft (Windows Server), IBM (WebSphere), BEA (WebLogic), Oracle, and JBoss.

Also, because the customs CIS servers have highly sensitive data and their availability is considered critical for Customs operations, it will be specifically protected from unwanted access or malicious attacks by a host-based Intrusion Protection System (HIPS) in addition to the upstream IPS's and firewalls. The CIS HIPS works much like the one described earlier for the secure mail server, but it is tuned and focused especially for the types of threats posed to the CIS servers; thus it will be more effective in removing such specific customs processing threats.

HIPS are used to protect servers through software that runs between your system's applications and the OS kernel. The software is preconfigured to determine the protection rules based on intrusion and attack signatures. The HIPS will catch suspicious activity on the system and then, depending on the predefined rules, it will either block or allow the event to happen. HIPS monitors activities such as application or data requests, network connection attempts, and read or write attempts, etc.

While not a complete list, some examples of appropriate host-based IPS (HIPS) vendors that can be used as an initial list for further investigation and analysis in filling this need are – McAfee, Cisco, Sana, and Symantec.

- Reporting Server – This report generation and management server will primarily work with the contents of the CIS data warehouse in order to generate Customs processing status, management, and planning reports for both internal and external usage. The breadth of these reports will heavily depend upon the planning and growth of the CIS data warehouse. Thus, the development of the overall database management and data warehouse solution, as well as the supporting data model and the “trickle feed” of selected CIS data automatically and periodically to the data warehouse, should be closely coordinated with the Customs internal and external reporting needs.

While not a complete list, some examples of appropriate report generation and management server vendors that can be used as an initial list for further investigation and analysis in filling these needs are – Microsoft, Crystal Reports (XI), Coremetrics, Imceda, NetIQ, and Omniture.

- Centralized Customs Operational Database (COD) Servers with host-based IPS – The new centralized customs system that will replace the legacy CCAS will require a new supporting centralized database management solution, and also provides an opportunity to update / improve the customs data model for current operational and data warehouse needs.

While not a complete list, some examples of appropriate content management and file server vendors that can be used as an initial list for further investigation and analysis in filling this need are – Microsoft, Oracle, Interwoven, and Accumo.

Also, as noted above for the CIS HIPS, some examples of appropriate host-based IPS vendors that can be used as an initial list for further investigation and analysis in filling this need are – McAfee, Cisco, Sana, and Symantec. This choice does not

need to be the same HIPS vendor that was chosen for the secure e-mail server, but should likely be the same as that was chosen for the new CIS.

- ❑ Centralized Customs Data Warehouse (CDW) – The CIS data warehouse should ideally represent the same database management technology and vendor choice for customs processing. Thus, the same list generally applies and should be coordinated with the related decisions that are currently being made for the new CIS vendor and its supporting database management solution and vendor.
- ❑ Network Attached Storage (NAS) Group – Customs will require large amounts of fast storage devices for both the Customs Operational Database (COD) as well as the Customs Data Warehouse (CDW). This storage should not only be large and fast, but should also include functionality to enhance availability, reliability, monitoring, backup, and disaster recovery.

An additional “like to have” as opposed to “must have” requirement for this NAS is that it be based upon the same operating system (OS) technology used elsewhere in the Customs Enterprise Architecture. Thus, this should be based upon either Microsoft Windows Server or Linux, because there will likely be other Customs components based on one or both of these (e.g. depending upon the CIS application server and database server technologies chosen, among others). This will aid in the consistency of technical skills needed across multiple components (and less additional training). In the case of storage devices, Linux has also established itself as an inexpensive, fast OS with little overhead. Arguably, this gives it an advantage over Microsoft Windows, which is more expensive (Linux is very cheap or free) and is known to have more overhead (everything else such as hardware being equal, the NAS may be slower with Windows).

While not a complete list, some examples of appropriate NAS vendors that can be used as an initial list for further investigation and analysis in filling this need are – Hewlett-Packard, IBM, FalconStore, Tandberg Data, Maxtor, and Mountain View Data, Procom Technology, Quantum SnapServer, RaidZone, Spinnaker Networks, and Advanced Media Services.

2.4.4. Main Site Other Infrastructure Components

Note that in order to complete the details of the infrastructure components for the main customs processing site, we must also include the following:

- ❑ Fast Ethernet Switches of the Site Users Access Zone – These are typical high-speed LAN 100 Megabit per second (100-Mbps, 100BaseT) Ethernet switches such as those discussed earlier for the Internet Access Zone. In the case of the Egyptian Customs network, 100BaseT4 switches are required for four pairs of (voice or) data-grade Category 5 wiring. Note that Gigabit switches (1,000 Mbps) may also be considered, but at this time these would be “overkill” for the anticipated Egyptian Customs processing needs.

While not a complete list, some examples of appropriate fast Ethernet switch vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, NetGear, D-Link, 3Com, and TrendWare.

- ❑ Intranet Edge Router – This is the Ethernet Router at the perimeter of the Intranet Zone and Intranet / Extranet Zone for Intranet access to the Customs site network. It is the concentration point for all Intranet transactions from other (main and secondary) customs sites, and is the only access point directly to the main customs Site Internal Access Zone. Unlike the Internet / Extranet Edge Router described earlier (for the Internet / Extranet Zone), this edge router does not require an IOS firewall, IDS, or context-based access control.

While not a complete list, some examples of appropriate edge router vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, Juniper, Laurel, and Lucent.

2.5. Secondary Customs Sites Architecture Solution

The recommended solution for the architecture of the secondary customs sites is shown below in Figure 2. This architecture will apply to the customs sites at the Cairo Airport, Misr Station, Danietta, Dekhaila, Sohkna, Suez, and possibly at Port Said (under consideration), which is to be determined since this may be assigned to become a main customs processing site instead.

In describing the details of the Secondary Customs Sites Reference Architecture, we begin by explaining the architectural goals and an overview of the secondary customs sites solution. Following this, we continue with an explanation of the details for each zone / domain that comprises the secondary customs sites architecture as shown in Figure 2 below.

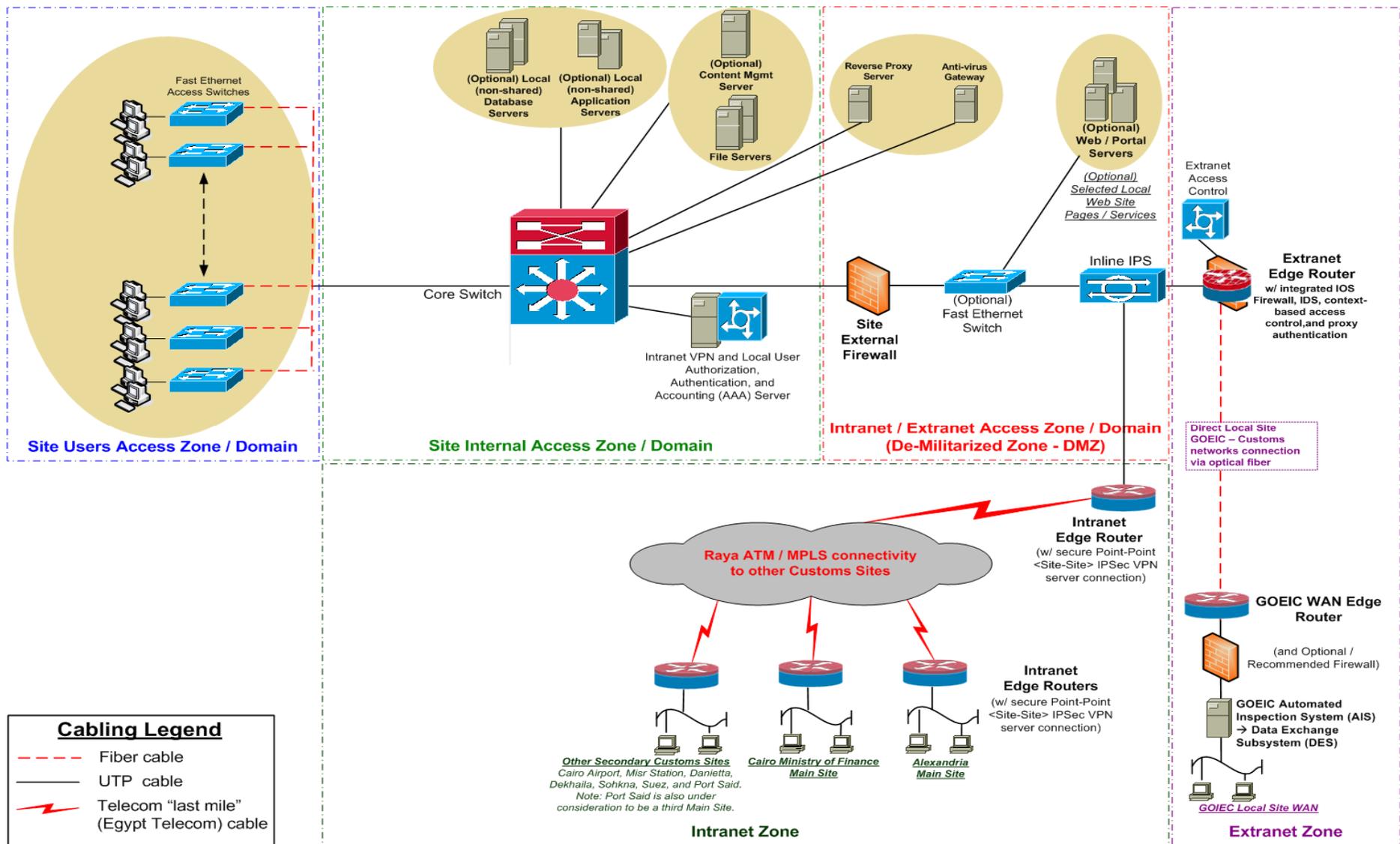


Figure 2. Secondary Customs Sites Reference Architecture

2.6. Secondary Customs Sites Architectural Goals

The primary architectural goals of the secondary customs processing sites are to:

- 1) Provide local customs site access to and efficient connectivity with the centralized, shared customs processing functions and components of the appropriate main customs processing site, including the centralized Customs Information System (CIS), Customs Operational Database (COD), Customs Data Warehouse (CDW), customs management reporting, and the Customs Data Interchange (CDI) for external organizations' consumption of customs data. These functions will not strategically be performed at secondary sites even though some are done there today. Hence, the secondary sites will become consumers of these main site services when they come on-line.

- 2) Provide local site access to and efficient connectivity with the centralized, shared services workflow capabilities of the appropriate main site.

Supporting the primary customs processing functions, the main sites will also host primary workflow management capabilities, including business rules, transaction queuing capabilities, and an enterprise services bus (ESB). The secondary sites will indirectly become consumers of these services when the centralized, shared main site customs processing functions come on-line.

- 3) Provide an implementation migration path that will continue to support the current distributed customs processing at the secondary sites until the centralized, shared functions are ready to be hosted only at the main sites.

While this architectural goal also applies to the main sites, it implies more current responsibilities for the secondary sites while customs processing and reference data sharing (i.e. with GOEIC) continues to be locally in advance of implementing the new CIS and centralized architecture.

- 4) Provide local site access to and efficient connectivity with other non-customs-related centralized, shared services and components at the appropriate main site, including e-mail, Internet access, intranet management, customs network and data security, and internal and external web and portal services.

These organizational IT infrastructure components facilitate business within the main sites and between all (main and secondary) sites, ensuring the appropriate level of communications and security is maintained for all customs user groups.

- 5) Potentially provide failover, disaster recovery, load balancing, and backup services for selected other secondary site(s) as needed.

These goals may be considered high level functional requirements for the secondary customs processing sites, such that a combination of these with the details outlined in subsequent sections may become functional requirements for developing technical specifications as part of a request for proposal (RFP) and related vendor proposals for all or part of the overall secondary site solution.

2.7. Secondary Customs Sites Solution Overview

The secondary customs sites will achieve the goals listed above by applying an architecture that distributes the functional customs processing and access to the site's functions into appropriate security zones. Each zone within the secondary site will be established as a local domain within the site's architecture, and each zone is delineated by a different "trust level" than its adjacent zones. Hence, there are security mechanisms that will be established at the perimeter between the zones with different trust levels in addition to the security mechanisms established within selected zones, in order to protect sensitive data or

functions that would otherwise be at risk from unsecured transaction requests originating from a zone with a lower trust level.

Descriptions of the applicable security zones / domains for the secondary customs processing sites are (right to left, top to bottom in Figure 2):

- Extranet Zone – This zone could include user groups and transactions that must be treated as the highest risk for the secondary customs sites, because it may contain public traffic for which there is no control before it enters the zones of the customs site. In the case of valid users and transactions originating from the Extranet Zone, a secure and encrypted site-to-site virtual private network (VPN) Extranet will be established between the local GOEIC organization and the secondary customs site. This will initially be to acquire customs reference data directly from the current local CCAS database. Eventually this local data acquisition will migrate to the centralized CIS customs data at the main sites, but for which this local customs site access will be extended into the Customs Intranet for this access.

Note that unlike the main sites, which have an Internet / Extranet Zone, the secondary sites have this more focused Extranet-only zone. Hence, secondary sites do not allow direct Internet, PSTN, or remote users access, as do the main sites. When this access is needed by the secondary sites (i.e. Internet access for e-mail, etc.; or remote user access to customs processing / data), this is accomplished via services provided through the main site (which has the necessary higher levels of security especially for these types of functions).

- Intranet / Extranet Access Zone (or De-Militarization Zone, DMZ) – This zone includes all components to directly handle transactions entering from the Intranet or Extranet zones. It is the only access point to the secondary customs site from either of these zones, and is initially intended to only allow the following access for transactions:
 - 1) GOEIC fully secure VPN-enabled transactions to enable back-end customs processing, and in particular to customs reference data, communications through the secure Extranet VPN channel; and
 - 2) Customs secure Intranet VPN connectivity to all other main and secondary sites via the Raya MPLS network.
- Site Internal Access Zone – This zone hosts all back-end site processing functions and components, which in the case of secondary sites will become rather small compared to the main sites (since the main sites will host the centralized, shared CIS, COD, CDW, customs management reporting, and the CDI for external customs data exchange). This is the strategic view. However, in the short-term, while the CCAS legacy customs system is still in operation, customs processing will continue at the secondary site in its current distributed fashion, and will also supply the necessary customs data to GOEIC.

Thus, the only long-term transaction requests that will be processed in this zone are those that have:

- 1) Originated from the Extranet Zone and cleared the relevant security mechanisms (VPN encryption / decryption, firewall, Extranet Access Control, and the inline Network Intrusion Protection System <NIPS>);
- 2) Originated from the local Site Users Access Zone (see below) and cleared the AAA server; or
- 3) Originated from the Customs Intranet Zone (see below) and cleared the Intranet-related security mechanisms (VPN encryption / decryption, NIPS, and the AAA server).

- Site Users Access Zone – This zone contains all the local site user workstations. This generally means just desktops at the secondary site, but could eventually be expanded to also include selected laptops and handheld devices at the site, as well as Ethernet switches, hubs, and wireless local area network (WLAN) components (to be determined). However, for the purposes of this the proposed solution, and in the interest of promoting a highly secure customs processing environment, this architecture only recommends desktop workstations connected by Ethernet switches at the secondary sites. Allowing any of these other access device types has the potential to expose the otherwise secure customs network. It is recommended to not allow these other device types initially and only allow these later on when further appropriate security mechanisms are put into place to manage these.

For example, it is anticipated that handheld device access via WLAN could be prudent for selected customs functions at a later date (e.g. to process radio frequency identification <RFID> tags at loading docks or in customs goods warehouses). In advance of instituting such access and functionality, an encrypted, secure WLAN would need to be established, and processes would need to be created and managed for the inventory, software, and location management of the limited number of allowed handheld devices. This would all occur within the Site Users Access Zone.

- Intranet Zone – This zone is strictly for the Egyptian Customs Intranet (ECI), which includes the Raya managed MPLS network as well as the Egypt Telecom “last mile” or connectivity that provides the primary data communications between all main and secondary customs sites. It is intended to only allow security-controlled and filtered transactions for authorized customs users to enable back-end customs processing and communications through a fully secure site-to-site VPN channel.

Each of these zones / domains is further detailed by its user groups and infrastructure components in separate subsequent sections below.

2.7.1. Secondary Extranet Zone User Groups and Infrastructure Components

The only user group of the Extranet Zone is the GOEIC WAN. Hence, GOEIC access to the customs site is an authorized secure site-to-site VPN connection over a local site fiber optic cable for the purpose of acquiring selected customs data that will be regularly processed by the GOEIC Automated Inspection System (AIS). It should be noted that both main and secondary customs processing sites allow this type of GOEIC VPN access.

Note that in the future, while the GOEIC connectivity to customs will continue to come through each (main and secondary) site’s Extranet Zone, the actual customs data will be retrieved only from the main customs sites. Thus, GOEIC’s request for customs data that originates from a secondary site will actually be processed at the appropriate main site that hosts the centralized Customs Information System processing for that secondary site.

The infrastructure components and related processes of the Extranet Zone are as follows:

- VPN software and security token for GOEIC – In order to facilitate a secure VPN connection for the GOEIC WAN, as well as to control this VPN access, the appropriate VPN software and security token will be utilized. The customs VPN software licenses and physical tokens will be inventory managed in order to ensure that it is always known who has access to the customs site processing and data.

Ideally the same secure tokens utilized by the main sites and described earlier will also be used at the secondary sites for GOEIC (see section 2.4.1 for more details about the VPN software and security tokens). These will be used when the authorized GOEIC server is logging into the customs network. For the purposes of

this report, we are referring to one of the most common and portable of the security token options, the dongle, and this may either be external (e.g. number is read by the user to be entered) or a USB dongle to be inserted into the workstation. Other types, however, may be considered if desirable by Egyptian Customs. Note that these secure tokens, like local site physical security access, will eventually be replaced by some form of biometric data validation.

The appropriate VPN software will establish a secure channel between the GOEIC server and the customs site. As stated earlier, IPSec is widely considered more secure than SSL for VPNs when used with MPLS networks, so for the purposes of this report, we concentrate only on a VPN implementation utilizing IPSec.

While not a complete list, some examples of IPSec VPN software vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, NetGear, SonicWALL, WatchGuard, Symantec, Enterasys, and FireBox. Note that the customs site VPN software and the RA user client VPN software (on the remote workstation) needs to be compatible, so it is recommended that these be from the same vendor. This will also ensure no support gaps in the overall VPN solution.

Similarly, some examples of secure physical tokens are listed here by vendor, which can be used for the selected VPN solution as an initial list for further investigation and analysis in filling this need are – RSA, Entrust, ID Control, Matrix, and Omnikey. A secure token can take the form of a smart card, ID, USB pen drive, or a dongle

- Extranet Edge Router – This is the Ethernet Router at the perimeter of the customs site network for non-Customs access, in this case only for GOEIC. It is the only access point for non-Customs users (in this case, just GOEIC) to the customs secondary site Intranet Access Zone or DMZ. This edge router should ideally include an integrated Internetwork Operating System (IOS) firewall, Intrusion Detection System (IDS), context-based access control, and proxy authentication. Otherwise, these supporting functions will need to be provided by an adjacent device or server (e.g. Extranet Access Control, see below). Also, while this function will be rather simple when only allowing one or a small number of GOEIC accesses initially, this gives the secondary site additional flexibility for potential remote user access in the future.

While not a complete list, some examples of appropriate edge router vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, Juniper, Laurel, and Lucent.

- Extranet Access Control – This access control software may either be integrated into the Extranet Edge Router or provided on an adjacent device / server connected to the router. It provides the first line of defense for the Extranet VPN by controlling VPN user access authentication, as well as context-based access control and proxy authentication if any of these services are not integrated into the Extranet Edge Router. While this function will be rather simple when only allowing one or a small number of GOEIC accesses initially, this gives secondary sites the additional flexibility to consider potential remote user access in the future.
- GOEIC-to-Customs site fiber cable connection – This is an optical fiber cable hardware connection between the GOEIC WAN Edge Router and the customs site Extranet Edge Router. In some secondary sites, this connection already exists but may need to be secured by firewalls on both the customs network side and GOEIC network side of the connection. In other sites, the fiber cable either needs to be initially laid or replaced in order to establish a working fiber optic connection (and then appropriately firewalled on both sides of the connection).

- GOEIC WAN and Edge Router – The GOEIC WAN encompasses all the local site systems and automated processes, including the Automated Inspection System (AIS). This system requires information from the Customs Information System (CIS) database and will receive this data via a secure VPN channel between the GOEIC WAN Edge Router and the secondary customs site Extranet Edge Router (over the fiber cable physical connection). Within the GOEIC WAN, the Data Exchange Subsystem (DES) of the AIS will translate the XML data acquired from the CIS database.

Note that the secondary sites do not have a CIS. It is the strategic direction that CIS processing and data will be centralized at the customs main sites on behalf of all the secondary customs sites. In the future, while the GOEIC connectivity to customs will continue to come through each (main and secondary) site's Extranet Zone, the actual customs data will be retrieved only from the main customs sites. Thus, GOEIC's request for customs data that originates from a secondary site will actually be processed at the appropriate main site that hosts the centralized Customs Information System processing for that secondary site. However, in the short-term the legacy CCAS will continue to process customs data and share selected customs reference data with GOEIC locally.

As suggested in the GOEIC WAN for main sites, there should also be a firewall established at the GOEIC Edge Router at secondary sites in order to protect the AIS and DES from unwanted attacks UNLESS this router only services the fiber connection between GOEIC and the customs site (i.e. the router has no other connection). For the purposes of this report, it is assumed that the GOEIC WAN Edge Router services other external transaction requests and should be treated as an internet / extranet edge router with the appropriate firewall (and further anti-virus and IPS) protections.

2.7.2. Secondary Intranet / Extranet Access Zone (DMZ) User Groups and Infrastructure Components

The user groups of the Intranet / Extranet Access Zone are as follows:

- GOEIC wide area network (WAN) – The GOEIC data transaction requests will have already been validated and filtered by the Extranet Edge Router, firewall, and External Access Control of the Extranet Zone prior to entering this more secure zone.

Since GOEIC transactions are intended to gather data from the Customs database and data warehouse, and these components reside within the Site Internal Access Zone, it is intended that valid GOEIC transaction requests will traverse past the Intranet / Extranet Access Zone to be processed in this more secure zone, while this is still done at each site (i.e. until the centralized CIS is implemented). At the later time that the centralized, shared CIS functions and data are implemented at the main customs processing sites, such GOEIC requests will be directed to the appropriate main site's Internet / Extranet Edge Router upon being validated by the secondary site Extranet Edge Router and Access Control.

The routing of GOEIC transactions both to the Site Internal Access Zone components and for redirection for main site processing may be assisted by the Intranet Access Zone's reverse proxy server to determine which destination server is appropriate to field each transaction.

- Local Site Users – In the short term, local site users will also use the Customs processing functions and data of the local Site Internal Access Zone. In the long run, these users will use the centralized CIS functions and data of the main site's

Site Internal Access Zone, as well as the e-mail and secure web services of the main site's Internet Access Zone.

The infrastructure components and related processes of the Intranet / Extranet Access Zone are as follows (right to left and bottom to top in Figure 2):

- Inline Network Intrusion Protection System (IPS or NIPS) – This is the first line of defense against all external attacks (e.g. viruses, worms, denial-of-service <DoS>, etc.) and other unwanted accesses (e.g. invalid usage) within the Intranet / Extranet Access Zone.

Thus, at this point, requests originating from the Extranet will have cleared the Extranet Edge Router, as well as the firewall, IDS, and Extranet Access Control components of the Extranet Zone. It is now the responsibility of the NIPS to review all incoming transactions through deep packet inspection in search of such unwanted usage, and provide alerts or shut down access as deemed appropriate. Similarly, requests originating from the Customs Intranet will have passed through a secure site-to-site encrypted VPN channel prior to being processed by the NIPS.

Egyptian Customs must monitor their networks for unauthorized intrusions, as hackers will be interested in crashing systems, deleting and / or manipulating data, and stealing data. Due to the sophistication of hackers, Customs needs to go beyond properly configuring servers and implementing firewalls. Instead, network intrusion software is another important tool for preventing unauthorized access to the Customs networks and systems by monitoring networks and identifying suspicious and malicious activity. Customs needs to acquire and implement network intrusion software as soon as possible and have key IT staff trained on how to use it properly. Note that the need for strong firewall and IPS technologies is now greater at the secondary sites than may be in the future. The reason is that there is still sensitive customs functions and data processing at the secondary sites, which will be phased out in lieu of the future centralized, shared CIS processing, and COD and CDW data, only at main sites in the future.

A highly functioning stateful IPS will correctly identify patterns of transactions and embedded data via dynamic rule updates in order to determine the nature of usages to either allow or disallow their downstream processing. Hence, only transaction requests that are allowed by the IPS will be further processed by the (optional) web / portal servers, reverse proxy server, or by components of the Site Internal Access Zone (e.g. the current CCAS and database, etc.).

While not a complete list, some examples of appropriate inline NIPS vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, Network Associates, Sana Security, ForeScout Technologies, StoneGate, TippingPoint, Enterasys, and IntruPro.

- Fast Ethernet Switch (Optional) – This is a general 100 Megabit per second (100-Mbps or 100BaseT) Ethernet switch intended for fast local area network (LAN) traffic routing. In the case of the Egyptian Customs network, a 100BaseT4 switch is desired because of its four pairs of data-grade Category 5 wiring. Note that Gigabit switches (1,000 Mbps) may also be considered, but at this time these are considered “overkill” for the anticipated Egyptian Customs processing needs.

Note that this fast Ethernet switch for the Intranet / Extranet Access Zone is optional and may only be needed if the optional web / portal servers are deployed.

While not a complete list, some examples of appropriate fast Ethernet switch vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, NetGear, D-Link, 3Com, and TrendWare.

- Site External Firewall – This is a combination OSI Layers 3 (Network), 4 (Transport), and 7 (Application) firewall intended enforce policies for transactions that involve secure services within the Site Internal Access Zone (i.e. temporary CCAS services, etc.). See section 2.4.2 for more details in regarding to the choice of an appropriate firewall technology and vendor.

While not a complete list, some examples of appropriate firewall vendors that can be used as an initial list for further investigation and analysis in filling this need are – Microsoft, Checkpoint, Cisco, Clavister, CheckPoint, and WatchGuard. Initial analysis has uncovered that –

- Two of the most advanced application-layer firewalls are CheckPoint's FireWall-1 and Microsoft's ISA Server
- Cisco's PIX firewall, the most popular hardware firewall, is very good at packet filtering; however, if you add application-layer filtering capabilities via add-ons, there may be performance degradation
- WatchGuard Technologies has recently added new features to its line of firewalls and provides some of the best application-layer protection amongst hardware firewalls.

- Web / Portal Servers (Optional) – These may be standard web servers (i.e. computers on the World Wide Web that store HTML documents which can be retrieved via a web browser), portal servers that work with a particular back-end platform (i.e. Microsoft, Oracle, etc.), or a combination of these, each hosting selected web services. However, it is recommended that a standard web server platform be adopted for all Customs non- or partially-secure web services. In the case of secondary sites, this simply means that if the site serves pages that will be used via the customs main web site (and web servers) or site internal web pages are used by local users.

Fully secure, encrypted web services will be served by the web / portal servers of the Main site, and these may be provided via the same web server platform and / or via portal servers that augment the back-end platform and processes. For example, if Oracle is adopted as the strategic database and data warehouse platform for Customs data and the new CIS, then it will be more efficient to deploy Oracle Portal Services for access to selected data. Similarly, if Microsoft SQL Server is adopted as the strategic data platform, then MS SharePoint Portal will be a logical choice for selected portal services.

While not a complete list, some examples of appropriate web server vendors that can be used if it is decided to have web / portal servers at the secondary site as an initial list for further investigation and analysis in filling this need are – Microsoft (IIS), Apache, Covalent, Roxen, Servotec, Xitami, and LightSpeed.

The two most prevalent web servers in the industry are Microsoft IIS and the Apache Web Server. These are compared and contrasted earlier in this document in Table 1 of section 2.4.2.

- Anti-Virus Gateway – Such an enterprise-level anti-virus gateway will provide high-performance, comprehensive, multi-layered protection against viruses, spam, and unwanted email and web content at the Internet gateway. A highly functioning anti-virus gateway will provide the following features:
 - Offers multi-layered spam prevention by combining blacklists and heuristic detection with whitelists in order to maximize detection and minimize false positives

- Provides secure remote management, advanced outbreak alerting, and concise reporting to view key performance and scanning metrics and overall system status
- Enables transparent virus definition and scan engine updates without restarting services or reinstalling software
- Delivers scalable, high-performance scanning with minimal network impact
- Includes scheduled delivery of antivirus and URL filter list updates, ensuring up-to-date protection

While not a complete list, some examples of appropriate anti-virus gateway vendors that can be used as an initial list for further investigation and analysis in filling this need are – Symantec, Trend Micro, Sybari, McAfee, Microworld, GFI, Finjan, F-Secure, Esset, Computer Associates, and Sophos.

- Reverse Proxy Server – This may be a separate proxy server, or may be a feature included with the external firewall software, as is becoming a trend amongst vendors. Thus, an advantageous choice of an external firewall that also has reverse proxy capabilities will reduce the need for a separate server / device for this purpose.

In its simplest form, a reverse proxy server is a layer that sits between a local area network (LAN) and an external network such as the Internet. The proxy server serves several needs, including –

- Enable several servers to share a single Internet connection by accepting and forwarding requests from the client (end user and GOEIC) applications
- Regulate (allowing or disallowing) certain communications with the outside world through site filtering
- Conserve bandwidth and increase network efficiency by caching content for repeated local delivery

As mentioned above, the reverse proxy server as a stand-alone product is becoming an endangered species, and it is more likely that we will solve this need in coordination with the selection of appropriate firewall servers. However, in the case that we need to seek reverse proxy specialist devices / software, here are some examples of reverse proxy server vendors that would be appropriate and can be used as an initial list for further investigation and analysis in filling this need are – Netegrity, Microsoft, Sun, and Squid.

2.7.3. Secondary Site Internal Access Zone User Groups and Infrastructure Components

The user groups of the Secondary Site Internal Access Zone are as follows:

- GOEIC wide area network (WAN) – The GOEIC transaction requests will have already been sufficiently validated and filtered by the security mechanisms of the Extranet and Intranet / Extranet Access (DMZ) zones prior to entering this most secure Customs processing zone. GOEIC transactions are intended to gather data from the CIS database and data warehouse, which all reside within the Site Internal Access Zone.

Since GOEIC transactions are intended to gather customs reference data from the Customs database and data warehouse, and these components reside within the Site Internal Access Zone, it is intended that valid GOEIC data transaction requests

will traverse past the Intranet / Extranet Access Zone to be processed in this more secure zone, while this is still done at each site (i.e. until the centralized CIS is implemented). At the later time that the centralized, shared CIS functions and data are implemented at the main customs processing sites, such GOEIC requests will be directed to the appropriate main site's Internet / Extranet Edge Router upon being validated by the secondary site Extranet Edge Router and Access Control.

The routing of GOEIC transactions both to the Site Internal Access Zone components and for redirection for main site processing may be assisted by the Intranet Access Zone's reverse proxy server to determine which destination server is appropriate to field each transaction.

- ❑ Local Site Users – Local site users will also use the CIS functions and data of the Site Internal Access Zone. Since transaction requests from site users will originate from the secure Site Users Access Zone (far left of Figure 2), there are generally no additional security mechanisms required within this zone.

In the short term, local site users will also use the Customs processing functions and data of the local Site Internal Access Zone. In the long run, these users will use the centralized CIS functions and data of the main site's Site Internal Access Zone, as well as the e-mail and secure web services of the main site's Internet Access Zone.

- ❑ Customs Intranet Users – Customs processing users located at secondary customs sites will access the CIS functions and data via the Intranet Edge Router that connects to the appropriate main customs processing site (as well as to all other main and secondary sites). The primary process for which the supporting main site would use with this secondary customs processing site is to coordinate with this secondary site for Customs data synchronization and backup for selected data (not full view). However, it is understood that all master customs data is only maintained at the main sites.

The infrastructure components and related processes of the Internal Access Zone are as follows (right to left and bottom to top in Figure 2):

- ❑ Intranet VPN and Local User AAA Server – This is typical AAA server software to handle user requests for access to (Customs internal) computer resources and to provide authentication, authorization, and accounting services for the Customs enterprise. In this case, the AAA services are to facilitate the authorization and authentication of valid local users and valid remote Intranet users of the Customs processes and data. Since this is a secondary site, the access to Customs processing and data is only a short-term need, since the long-term direction for customs processing is to implement the centralized, shared CIS only at main sites. At that point, all secondary sites would convert to being consumers of the main site CIS processing and data.

While not a complete list, some examples of appropriate AAA server vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, Hewlett-Packard, ActiveIdentity, Telecount, and Merit.

- ❑ Core Switch – This core switch is intended to do the “heavy lifting” of the switching between all the various servers that reside within the Internal Access Zone on behalf of local site users, Intranet Customs users, and GOEIC usage. Note that the GOEIC usage of secondary sites in particular will mostly be going away when the new CIS is implemented.

On behalf of the local end users, this switch provides the appropriate switching between the relevant servers for Customs content, file, and (optional) data access. However, for Intranet user requests that are originating from the less secure Intranet Zone, the site external firewall and NIPS of the Intranet / Extranet Access Zone are

utilized for additional security before switching the request within the Internal Access Zone.

While not a complete list, some examples of appropriate core switch vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, PMC-Sierra, Extreme Networks, Enterasys, Force10 Networks, and Foundry Networks.

- Content Management Server (Optional) and File Servers – These servers will fill the secondary site optional needs for shared: 1) (optional) web page and document content management for the Egyptian Customs website and web services, 2) customs back-end document and image processing (optional), and 3) basic file management for all local customs sites users.

The content management server in particular is listed as optional here because it, like the Fast Ethernet Switch of the Intranet / Extranet Access Zone, may not be needed if it is decided to not distribute any web / portal server capabilities at the secondary sites.

While not a complete list, some examples of appropriate content and file management server vendors that can be used as an initial list for further investigation and analysis in filling these needs are – Microsoft, FileNet, Oracle, Interwoven, and Accumo. Also note that some of these vendors have particular strengths that make it possibly desirable to employ more than one Content Management solution (e.g. FileNet is particularly strong for document and image processing, while Microsoft Content Manager is stronger for web content management).

- Local (non-shared) Application Servers (Optional) – Application servers may be needed to serve local applications at certain secondary sites, and this will have to be determined on a case-by-case basis. It is assumed for the purposes of this report that such servers will either be based on a Java open source platform or a Microsoft platform. Hence, while not a complete list of the many available application server vendors, some example vendors that may be used as an initial list for further investigation and analysis are – Microsoft (Windows Server), IBM (WebSphere), BEA (WebLogic), Oracle, and JBoss.
- Centralized Customs Operational Database (COD) Servers with host-based IPS – The new centralized customs system that will replace the legacy CCAS will require a new supporting centralized database management solution, and also provides an opportunity to update / improve the customs data model for current operational and data warehouse needs.

While not a complete list, some examples of appropriate content management and file server vendors that can be used as an initial list for further investigation and analysis in filling this need are – Microsoft, Oracle, Interwoven, and Accumo.

Also, as noted above for the CIS HIPS, some examples of appropriate host-based IPS vendors that can be used as an initial list for further investigation and analysis in filling this need are – McAfee, Cisco, Sana, and Symantec. This choice does not need to be the same HIPS vendor that was chosen for the secure e-mail server, but should likely be the same as that was chosen for the new CIS.

2.7.4. Secondary Site Other Infrastructure Components

Note that in order to complete the details of the infrastructure components for the secondary customs processing site, we must also include the following:

- Fast Ethernet Switches of the Site Users Access Zone – These are typical high-speed LAN 100 Megabit per second (100-Mbps, 100BaseT) Ethernet switches such

as those discussed earlier for the Internet Access Zone. In the case of the Egyptian Customs network, 100BaseT4 switches are required for four pairs of (voice or) data-grade Category 5 wiring. Note that Gigabit switches (1,000 Mbps) may also be considered, but at this time these would be “overkill” for the anticipated Egyptian Customs processing needs.

While not a complete list, some examples of appropriate fast Ethernet switch vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, NetGear, D-Link, 3Com, and TrendWare.

- Intranet Edge Router – This is the Ethernet Router at the perimeter of the Intranet Zone and Intranet / Extranet Zone for Intranet access to the Customs site network. It is the concentration point for all Intranet transactions from other (main and secondary) customs sites, and is the only access point directly to the main customs Site Internal Access Zone. Unlike the Internet / Extranet Edge Router described earlier (for the Internet / Extranet Zone), this edge router does not require an IOS firewall, IDS, or context-based access control.

While not a complete list, some examples of appropriate edge router vendors that can be used as an initial list for further investigation and analysis in filling this need are – Cisco, Juniper, Laurel, and Lucent.

3. OTHER ARCHITECTURAL CONSIDERATIONS

3.1. Developing a More Robust and Modern Enterprise Architecture

The current Customs enterprise architecture is not very robust. It was primarily developed to support the outdated Customs Commission Automated System (CCAS), which has significant design flaws, considering the newer technology that is available today. Part of the problem has been a lack of IT infrastructure investment by Egyptian Customs over the years.

A significant architectural issue is that the CCAS was implemented as a distributed system with independent processing and databases running in several “main” Customs locations. While this system architecture made sense when originally developed in 1998 (i.e. because of the state of tools and data communications at that time), programming tools and system technologies are now available which would:

1. Enable the development and implementation of a much more robust and centralized system and database architecture.
2. Provide additional customs processing application functionality and a flexible modular application architecture that can be configured for the Egyptian Customs functional requirements.
3. Support a more robust Customs data model to address all internal and external user groups, as well as the electronic exchange of selected Customs data with government (e.g. GOEIC) and business partners (e.g. traders and banks).
4. Better utilize the available network capacity of the recently upgraded Customs Wide Area Network (i.e. the Raya MPLS WAN).

Hence, the current distributed systems architecture does not avail itself for the data communications capabilities of the current WAN. Also, application server technologies should be employed to centralize the system, creating a scalable solution that properly utilizes the WAN. Customs should upgrade to a new Customs system that is a web-based n-tier model, based upon proper application server technology, and centralize hosting of the new system at the main site (primary and backup) locations. This is beyond the planned scope for the Interim Modernization Phase, so follow-on planning should begin as soon as possible.

Also, the development tool used to create the CCAS user application is PowerBuilder, a product that is part of the Sybase family. Using this tool made sense originally, since the original CCAS was based on a Sybase database management system. If the database management system is changed for the Customs Commission Automated System, as this document suggests, then the application development tool should also be changed to a more appropriate and perhaps more mainstream development tool.

The Interim Modernization Phase only addresses basic enterprise architecture issues, such as creating central data processing centers in Cairo and Alexandria, and implementing a centralized database for the CCAS. The whole enterprise architecture for Customs, however, will need to be changed, specifically including the implementation of a new Customs Information System (CIS) based upon an n-tier architecture model. The reason this is not being addressed during the Interim Modernization Phase is that the new CIS vendor has not been identified yet. The interim plans for enhancing the Customs enterprise architecture make sense, but much more needs to be done in advance of and when a new CIS is implemented.

In the future, the new CIS envisioned should be a web-based application. All authorized users should be able to log into the new Customs system through a web browser. The main benefits of a web-based system include:

- No application software needs to be installed, and therefore, there is no need for managing the installation of new versions of the user application (in other words, no version control).
- Web-based systems are highly scalable, using clustered application and system servers to manage user connections and store and retrieve data from the system. Servers can be added to the clusters depending on system demands.
- Technical support requirements are significantly reduced because users only need a working (and compliant) web-browser to access the system—in other words, there should not be any system failures on the client side. This means the technical support staff at Customs points will only need to provide basic PC technical support.

Most commercial customs packages are web-based, reflecting the trend in Customs organizations throughout the world towards adopting this technology.

A complement of IT systems is required for a smoothly operating customs organization. Egyptian Customs has logically focused on the core Customs Commission Automated System with additional support modules built into the core system for basic operations, including personnel, purchases, budget, suppliers and payroll modules. The Customs Commission Automated System, however, fails to meet international standards and should either be upgraded or replaced. TAPR-II will analyze the options for upgrading or replacing the CCAS, provide guidance and recommendations on the appropriate steps forward, and assist with implementation of the agreed solution. The other main systems also need to be addressed in order to modernize Egyptian Customs. The subsections below discuss the current situation with the Customs Commission Automated System, as well as single window, data warehouse, human resources and enterprise resource planning systems.

3.2. Addressing International Standards

The IT infrastructure of Egyptian Customs is currently only partially developed and needs significant improvement to comply with internationally accepted standards. Key deficiencies are apparent with the current CCAS, which must be rectified as part of the project to select and implement a new Customs Information System (CIS). According to numerous consultant reports and the Head of the IT Department, Mr. Abdel Radwan, the CCAS does not meet international standards for either system functionality or its data model.

The goals of the Interim Modernization Phase will address some enterprise architecture issues, but much more needs to be done to be ready to introduce a new CIS and to address international standards.

3.3. Utilizing the Customs Data Interchange (CDI)

The new reference architecture for the main sites advocates Data Exchange Servers for the Customs Data Interchange (CDI) within the Site Internal Access Zone. This will initially support the need for selected customs data in XML format to be delivered to the GOEIC organization.

However, if the CDI is established with the appropriate flexibility and configurability, then the main customs sites will also be prepared to serve data to and receive data from other government and business entity consumers or receive data (in alternative formats such as EDIFACT or XML schemas) in the future. For example, it is anticipated that Egyptian

Customs will need to: 1) receive electronic declarations and manifests from traders and brokers; 2) send electronic payments to banks; and 3) send electronic customs data processing reports to other government agencies.

3.4. Upgrading the Database Management System (DBMS)

Sybase 11.5 is currently used as the database management system for the CCAS, and it is currently being upgraded to Sybase 12.1.5 during the Interim Modernization Phase. However, Sybase is not a good strategic choice for a database platform to support the new CIS.

There are many issues that this database platform choice raises, including that it:

- ❑ Limits the choices of CIS vendors (must be built for and support Sybase implementations), and may also hinder the performance of the CIS data input / output (may require an additional layer of abstraction and/or a custom adapter). Most CIS vendors will have instead built their products for the DBMS market leaders Oracle, Microsoft SQL Server, and/or IBM DB2.
- ❑ Does not have a strong history of application program interfaces (APIs), data access adapters, and integration with an Enterprise Services Bus (ESB) for a service-oriented architecture (SOAs) such as the DBMS market leaders Oracle, Microsoft SQL Server, and IBM DB2.
- ❑ Does not provide immediately compatible and robust supporting data processing, exchange, reporting, and (portal) display services to the extent of the DBMS market leaders Oracle, Microsoft SQL Server, and IBM DB2.
- ❑ Has a much smaller pool of readily trained and skilled DBMS professionals than does the market leaders Oracle, Microsoft SQL Server, and IBM DB2
- ❑ Raises the question of Sybase's long-term viability amidst declining market share and profitability compared with the DBMS market leaders.

Thus, although no change should be made for the Interim Modernization Phase, upgrading or replacing the current CCAS will undoubtedly also require (or at least provide an opportunity for) changing to a more appropriate strategic DBMS for the future. Thus, it is recommended that either Oracle or Microsoft SQL Server would be a much better long-term choice at the time of implementing the new CIS.

3.5. Launching and Maintaining a Data Warehouse

Customs does not currently have a data warehouse. However, an initial step towards building a Customs Data Warehouse (CDW), the creation of a centralized database repository for this purpose, is in progress. A concern, though, is that this project is being executed out of sequence. It may create significant difficulties later by creating the CDW before the choices of CIS and DBMS are accomplished. To mitigate this risk, the CDW and data model designs should be revisited upon completing each of these related decisions.

Egyptian Customs is not ready to implement a proper data warehouse. The two key problems are that there is not a centralized database and the quality of data in the Customs Commission Automated System is reported to be very poor. Since a data warehouse amounts to a consolidated database and related tools for management reporting and data analysis, the lack of a central database prohibits the creation of a data warehouse at this time. Poor data quality from the Customs Commission Automated System will also drastically reduce or even eliminate any value in creating a data warehouse. This can be summarized as the garbage-in-garbage-out problem.

Egyptian Customs needs to focus first on creating a central database (which is in progress) and addressing the issues that contribute to poor data quality. There may be some problems with the design of the Customs Commission Automated System, but most of the data quality problems are probably caused by manually consolidating data (which is error prone) at the Alexandria IT Center and poor or inconsistently applied data entry procedures. Implementing a centralized database and a new Customs information system will not necessarily solve all of the data quality problems, and a complete reevaluation of data entry procedures needs to be part of the Customs reform process before a data warehouse is implemented.

Creation of a central database is a good initial step towards the creation of a data warehouse, and consolidating all operational data in a central location will also improve the efficiency of generating management reports. Egyptian Customs should acquire a management reporting tool, such as Crystal Reports, to facilitate and automate the creation and distribution of standard and ad hoc management reports. Customs should also train IT staff on basic data warehouse techniques and technologies that can be applied as soon as the central database is created. Specifically, multidimensional data marts can be created by trained IT professionals, and these data marts can be used for robust, flexible management reporting.

Even with the data quality problems highlighted above, Customs should go ahead immediately with the procurement process for services to build and implement a data warehouse. The procurement process will take many months, and building and implementing a data warehouse is at least a 6-month project if not more. This will give Customs satisfactory time to finish creating the central database and resolve the main data quality problems. The key point is to start resolving the data quality problems now. Building a data warehouse is also necessary to support the development of proper risk models (data for the risk models will come from the data warehouse), and therefore, the procurement process needs to start as soon as possible to support this activity. The hardware and software required to support a data warehouse include the following.

3.5.1. Acquiring Extract, Transform and Load (ETL) Tools

Extract, transform and load (ETL) tools have not been required up until now by Customs, because no data warehouse had been implemented. However, since this is going to happen in the near future, it would be useful to purchase an enterprise license to an ETL tool such as Ascential or Informatica in anticipation of the CDW's needs as well as the likely data conversion needs in order to migrate to a new DBMS and/or for the implementation of the CIS.

Data warehouse software solutions usually include tools that help manage and automate the process of extracting data from operational databases, transforming the data (to make it more intelligible or to eliminate inconsistencies) and loading data into the data warehouse. Customs does not currently have any extract, transform and load (ETL) tools and does not need them at this time, since there is no data warehouse. Basic reporting tools are all that is needed during the Interim Modernization Phase until the data quality issues are satisfactorily addressed and a data warehouse is created. ETL tools should be part of the data warehouse procurement.

3.5.2. Acquiring Online Analytical Processing (OLAP) Tools

No online analytical processing (OLAP) tools are currently being used by Customs. In the Interim Modernization Phase, it would be useful, however, to purchase an enterprise license for a management reporting tool to interrogate the centralized database that is being created. Note, however, that such a tool should be capable to work with the likely choices of strategic long-term DBMS in addition to the current Sybase platform.

Reporting tools can sometimes be considered OLAP tools, but these normally are a more advanced set of tools that create multidimensional data cubes and allow users to generate ad hoc customized reports easily. During the Interim Modernization Phase, it does not make sense to invest in this kind of tool. OLAP tools, however, should be part of the procurement for a data warehouse. Basic reporting tools will be sufficient for the interim phase.

There are also business intelligence tools that are related, but often considered a separate family of tools. These tools are much too sophisticated for serious consideration at this time. Intermediate OLAP tools are available that will provide significant benefit, can be realistically implemented and supported, and are significantly cheaper than these advanced tools.

3.6. Establishing Regular and Automated Data Backup and Recovery

Data backup and recovery is a critical function to ensure that data is not lost if there is a system failure and that systems can be restored after a disaster. Data backups are performed inconsistently ranging from daily to once a week. Although the fact that data backups are performed is a positive sign, Customs must backup databases daily, or data is likely to be lost when there are system failures. In the main Customs locations, data backups are stored on the main server and also on 20 GB tape, which is placed in a safe. For the smaller locations, the servers do not have enough disk space, so backups are only stored on 4 GB tapes and stored in a safe. To ensure daily backup, backups need to be automated and scheduled on the system servers. Clear policies and procedures also need to be created for data backup and recovery, and compliance audits should be performed periodically.

The data backup and recovery that is currently performed is only rudimentary. The goal at least at the main Customs locations should be 100% uptime. Currently, this is not possible if there is a major systems failure, and not much can be accomplished during the Interim Modernization Phase. Restoring data from tape in particular is slow, so this is not sufficient. In addition, the use of servers with RAID controllers helps protect against hard disk failure, but does not protect against software, processor and other potential failures. When a new Customs information system is implemented, Customs will need to implement full backup servers in Alexandria and Cairo (and possibly Port of Said), and also robust data backup and recovery systems, such as IBM's Tivoli Storage Manager or SteelEye Technology's LifeKeeper for Linux, in order to meet a goal of 100% uptime.

In addition to the proper hardware and software to maintain 100% uptime, Customs needs proper disaster recovery policies and procedures and should periodically perform disaster recovery tests to ensure that these policies and procedures are working properly.

As a note, centralization of data processing in Cairo and Alexandria and implementation of the new server clusters will help improve system reliability and uptime substantially. The server cluster configuration calls for two quad processor servers with external mass storage at both locations. This provides a secondary (backup) processing center and backup servers at both locations. This configuration is robust as long as the processing centers have enough processing power for daily operations. At the time of initial implementation, it is anticipated that this configuration is sufficient. If more processing power is needed, then additional servers can easily be added to the cluster.

3.7. Establishing Enterprise Workflow Management

The current enterprise architecture does not lend itself to a services-oriented architecture (SOA) as is a good fit for the functional requirements of a Customs data processing environment. This is true for many reasons, including the distributed CCAS architecture and the current choice for Sybase as the DBMS. Also for these reasons, the current architecture does not readily enable workflow management and business rules, which along with an

underlying SOA architecture is a natural fit for enabling such a workflow intensive environment as Customs that is driven by business rules for next steps in processing, routing, inspections, approvals, etc.

3.8. Establishing and Maintaining a Proper Website

Although the website is primarily informational, there are some key functional requirements that need to be considered. These requirements include:

- A content manager,
- Multilingual capabilities,
- Search, and
- Downloadable documents.

A content manager is needed to allow non-IT staff to update the website. The suggested content manager should have a user-friendly interface that allows users to update text, add links and attach downloadable documents. This is critical to ensure that content on the site is maintained properly and is current. Multilingual capabilities are also required because not all users will speak Arabic. English and probably French should be available. Implementing a multilingual website requires storing text labels in a database in order to easily switch from one language to another. Once multilingual capabilities are implemented, the remaining task is to translate text labels and update the appropriate database tables. Search is a standard feature on websites, and the main issue is updating the search engine index when updating the content of the site. The last key requirement is the ability to attach downloadable documents, such as forms, to the website. This capability must be part of the content manager. Of course, there are other website requirements, but these are the main ones that should not be overlooked.

Due to the importance of maintaining a public presence on the Internet 24/7, a backup server needs to be set up for hosting the website. This is particularly important for Customs because people living in different countries and time zones will often access the site outside of normal working hours in Egypt. Alternatively, the website could be hosted by an Internet service provider that supplies its own backup systems. Sometimes backup Web hosting services will even be supplied from a different country, such as a European country. The point is simply to make sure the website is always available. For the Interim Modernization Phase, Customs should either implement a backup server or pay for website hosting services.

3.9. Creating a Single Window Environment for Customers

The purpose of single window software is to have one customer user interface that is a portal to all needed information, instead of requiring customers to submit documents online (or manually) in multiple locations. Such single window software would then routes the documents to the appropriate organization for processing and approvals. It is a document workflow system that works in conjunction with an enterprise workflow management and business rules solution. For example, FileNet is a good document and image management product that comes with standard adapters for industry leading workflow management servers such as Microsoft BizTalk, IBM WebSphere, and Tibco (which in turn work with business rules engines such as BizTalk BRE, WebSphere BusinessBeans, and JRules to name a few).

Implementing this kind of software would reduce Customs clearance times substantially, because documents do not have to be reentered, time is not wasted due to the submission of documents to multiple locations or organizations, documents are automatically routed to

other organizations for processing when that is required, and the status of documents and feedback on the process can be obtained online.

Customs clearance times are currently averaging between 10 and 14 days in Egypt, which is unacceptable. Much of this delay is likely dead time during organizational handoffs involved in the clearance process, specifically Customs and GOIEC.

Implementing single window software will help, but cannot resolve all the delays currently experienced with Customs clearance. Processes also need to be reengineered to make them more efficient, and risk selection needs to be fully implemented so that documents which pass risk assessment will be processed automatically (with automatic notification) to the customer.

An interface with GOIEC has been implemented in Sohka, which is a step towards a single window system, but it does not interface with all control agencies. The system also does not automate the processing of documents. It only shares data between the systems for later processing. Thus, even with the implementation of this system, clearance times in Sohka have not improved substantially.

The USAID ATR project has prepared a tender for the design and implementation of core components of an Automated Inspection System (AIS) that would interface between the CCAS and the GOIEC AIS system¹. The completion of these core components is scheduled for July 2006, and the interface will be based on XML. However, the planned interface does not cover the other control agencies that are involved in Customs clearance and will need to be integrated with the CCAS and eventually the CIS. It is the intention of the Customs Data Interchange described earlier that such a flexible data exchange mechanism will be implemented to support GOIEC needs today and other agencies, etc. later.

Thus, Customs will still need to implement single window software to manage more efficiently its own processes and the interaction among Customs, other control agencies, and GOIEC. Single window systems for customs, such as TradeNet, should be further investigated. In short, the new Customs Information System (CIS) must include single window capabilities as part of the overall solution.

3.10. Improving the Network Environment

The Customs wide-area network (WAN) has been outsourced to Raya Holding, the top IT integrator in Egypt. The WAN is based on multi-protocol label switching (MPLS). This is a network protocol that maximizes performance by monitoring network traffic and routing data packets along the most efficient network path. Purchasing network services from a vendor is cost effective and reliable option, as long as there are capable vendors in the local market. The performance of the network has been satisfactory. However, future demands on the network are likely to lead to greater bandwidth requirements.

The Customs site networks are neither robust nor well managed. There are some key networking issues that should be addressed in the near future:

- *Upgrading Network Connections* – Some network connections to the main Customs locations, specifically to the MoF towers and the Alexandria port, should be upgraded.
- *Implementing Proxy Server and Firewall Software* – As new Customs locations are connected to the Internet, which has been proposed, proxy server and firewall software needs to be properly installed and configured.

¹ Other control agencies involved in the Customs clearance process include the Ministry of Interior Affairs, the Ministry of Foreign Affairs, the Ministry of Trade and the Ministry of Industry.

- *Upgrading Hubs to Switches for LANs* – Hubs need to be replaced with switches in order to increase data transfer speeds to 100 Mbps for PCs with 10/100 network interface cards.
- *Implementing Domains* – Domains need to be implemented for all LANs in order to restrict access to authorized users.

Addressing these issues will improve network performance and security. These and other networking issues are discussed in more detail below.

3.10.1. Upgrading the Site LANs

Customs LANs in most locations are in poor shape. The main problem is that hubs are still predominantly in use. While many hubs are capable of running at 10 or 100 Mbps, they can only run at the speed of the slowest network card attached to the LAN. Since Customs has over 400 old PCs with 10 Mbps network cards, this presents a significant problem. Either a large number of PCs cannot be connected to the LANs, or the LANs will only be able to run at 10 Mbps. The latter is the case throughout Customs. The solution is to replace the hubs with switches, particularly in the main Customs locations. The price of switches has come down tremendously over the last five to ten years, so this is not a very expensive proposition, and it will significantly improve the performance of the LANs.

Network domains need to be set up, and users need to be assigned logins and passwords. Establishing domains will help protect the Customs Commission Automated System because users will have to log into their domain before they can gain access to the system. When asked why this has not already been done, the IT staff at the Alexandria IT Center said there was only one person to set up all of the user accounts necessary, and this person did not have enough time. Clearly, more staff members need to be trained in network administration in order to establish and maintain network domains.

LAN refurbishment is a critical issue, particularly in the main Customs locations. A project to refurbish these LANs has been proposed, but funding for this project has not been identified. At a minimum, the hubs in these locations need to be replaced with fast Ethernet switches. The approximate number of hubs that need to be replaced is 50. Table 2 below highlights the estimated number of Fast Ethernet Switches needed by selected key (Main and selected Secondary) site locations.

Customs Locations	Quantity
Alexandria (main)	15
Cairo MoF (main)	13
Dekhaila	8
Port Said (possible main)	8
Suez	5

Table 2. Estimated Number of Switches Required for Main and some Secondary Sites

Domains also need to be set up for the LANs, as identified in the reference architectures, which will require hiring and/or training more staff to setup domains. Network administration is one of the main courses recommended in the Gap Analysis. Donors should consider funding training for this course, since it is an immediate priority.

3.10.2. Improving Enterprise Network Engineering and Security

The network considerations include all aspects of connectivity within and between sites. Thus, we consider the Raya MPLS Wide Area Network (WAN) that provides inter-site Customs processing communications as well as the Local Area Network (LAN) at each site.

3.10.2.1. Addressing End-to-End WAN Connectivity

An important aspect of the WAN, in addition to the MPLS core provided by Raya Telecom, is the “last mile” of telecom connectivity between the MPLS WAN and the local LAN at each site. Even if we thoroughly trust the configuration and maintenance of the MPLS core network to be “spoof-proof” due to the advanced label switching technology, we cannot trust the “last mile” of traditional Telecom Egypt connectivity between the MPLS WAN and the local site’s LAN. In fact, Raya has pronounced that they have no responsibility for this leg of the network.

Thus, a secure encryption technology is required for the “entire WAN”, both over the MPLS main leg of this as well as the “last mile”. The best candidate for such secure encryption in terms of security, reliability, and manageability is IPSec.

3.10.2.2. Establishing Regular WAN Network Reporting

There are network reporting opportunities for which Customs is currently not taking advantage. For example, Raya will provide regular (monthly) reports for trouble ticketing if requested to do so. This is one way to ensure they are living up to an expected service level agreement (SLA). Also, Raya will provide a link to a customer web page to review the usage by the Customs sites of the MPLS WAN. Again, this opportunity for SLA validation and capacity planning is not being taken. This type of reporting should be assigned as a responsibility for a manager within the ECA IT organization to ensure the necessary service levels are being attained. The first step is to make use of these free reports, and then augment this information by internal network reporting with appropriate network monitoring tools.

3.10.3. Improving Technical Support for Managed Networks

Raya Holding is supplying the WAN with technical support. A service-level agreement (SLA) dictates the performance requirements for the WAN, and Raya is responsible for maintaining the required level of service. If Customs experiences a problem with the WAN, Customs calls Raya to get it resolved. Customs, however, does not have any network management software to monitor WAN performance to know if the SLA is being met. If significant network problems develop, Customs should consider implementing network management software. This should not be an issue during the Interim Modernization Phase, but would be a prudent step before the implementation of a new Customs information system, since a new system will definitely increase network traffic.

For LANs, Customs needs proper technical support. Organizing technical support for the site LANs is not difficult and should be provided internally. The key point is to make sure that the technical support staff members who are responsible for the LANs are properly trained.

3.10.4. Establishing Network Management Software

Customs is not currently using network management software to manage or monitor the wide-area network (WAN). The two main concerns are that bandwidth may not be used efficiently, causing bottlenecks, and there is no way to check if the service level agreement with Raya is being satisfied. The Operational Manager of the Alexandria IT Center is of the view that WAN performance was satisfactory, and if there is a problem, the IT staff call

Raya's call center to get the problem resolved. As long as performance is satisfactory, Customs does not really need to have network management software. The whole point of outsourcing network services is not to have to worry about these kinds of issues. For Customs having its own network management software is primarily an issue of maintaining a minimum comfortable level that the network is operating and being managed properly.

Although it is not critical, since there is a service level agreement for the WAN with Raya, Customs may want to monitor WAN performance. In the short run, Customs IT staff can use open source network management software. The Multi-Router Traffic Grapher that was already installed is also a good start for monitoring the WAN. In the long run, Customs may want to investigate using commercial products that are available, such as CiscoWorks, IBM's Tivoli, and Hewlett Packard's OpenView. If Customs decides that commercial products are needed, then training will be also required for the IT staff to properly use these tools.

3.11. Improving Customs Technical Support

The value of proper technical support should not be underestimated. Many IT projects fail during the implementation phase, and two of the main causes are poor training and technical support. When a user has a problem with a new system, technical support is the main resource for solving that problem. If the technical support team cannot fix the user's problem or explain how the problem should be dealt with, then the user is likely to revert back to the old way of doing business or do nothing at all. These outcomes are even more likely in an organization, such as Egyptian Customs, that does not have sophisticated computer users. Therefore, the technical support function needs to be very well developed before Customs embarks on any major new systems implementations.

In environments such as the one found at Egyptian Customs, technical support is often provided on an informal basis. Users tend to contact IT staff directly, usually based on personal relationships. This is counterproductive because there is no consistency to the support provided and queries from users can be very disruptive to the work of the IT staff—particularly during the rollout of new systems. Technical support needs to be carefully managed in order to ensure that it is provided properly and does not unduly disrupt the work of IT. Five key points for providing suitable technical support are:

- Sufficient staff must be assigned to the technical support function,
- Technical support staff must be suitably trained to provide high quality support,
- Technical support should be divided between four key areas—applications, hardware, software and networking—since most technical support staff will not have the skills to provide support in all areas,
- Onsite technical support should be available for troubleshooting basic problems, and
- A helpdesk function needs to be developed and appropriate software must be implemented to track reported problems and their resolution.

Besides the incredibly low number of Customs IT professionals in general, there is a lack of IT technical support staff, which needs to be addressed. Good technical support is critical to maintaining proper operation of IT systems. If users do not know how to use systems properly or systems generate errors, resources must be available to help the users. Otherwise, a significant amount of time will be wasted by users, leading to operational inefficiencies, and data quality will also probably suffer because data is not entered or is entered incorrectly.

While outsourcing technical support is an option and is currently done, Customs needs to make sure that the first line of technical support is properly implemented and managed locally. IT problems need to be reported to a central helpdesk, basic problems should be resolved by Customs technical support staff, and the resolution of problems needs to be tracked. Creating a helpdesk function is a key priority because it will increase the efficiency of technical support. But more importantly, it will track the types of problems users are experiencing in order to have a more coordinated approach to resolving IT problems. Development of the technical support function will take time, and in addition to creating a central helpdesk, IT staff members need to be identified, assigned and trained to provide basic IT technical support to users.

Technical support is a critical function for ensuring system sustainability. Providing proper technical support will increase Customs operational efficiency by reducing user downtime and also reinforce the implementation of new systems. The subsections below discuss the four main areas of technical support that should be provided, including Customs applications, hardware, software and networking.

In general technical support has been outsourced to vendors through maintenance contracts. This is a logical approach since there are not enough qualified staff to cover all technical support needs internally and also because the Customs Commission Automated System was developed by a vendor. Customs IT staff are only providing frontline technical support or first aid.

Technical support is a critical function to ensure proper implementation and use of systems, as well as system sustainability. Many IT system implementations fail or produce poor results because of insufficient technical support and training. Outsourcing is an effective way to ensure sufficient support, and this is typically what has been done by Egyptian Customs. Three key issues to keep in mind, regarding technical support contracts, include ensuring that technical support plans provide the level of support required, support coverage does not lapse because of contractual or funding issues, and the value of the service justifies its cost.

Even with technical support being largely outsourced to local vendors, Customs will need to provide frontline technical support. Solid frontline support contributes to smoother running operations because users will not always be inclined to call vendors for minor or small problems, and they will appreciate the option of being able to contact internal technical support staff. Frontline support should consist of a helpdesk and limited onsite support at the different Customs locations. The helpdesk should answer basic user questions, track all reported user problems and their status, elevate user problems to appropriate IT staff or the vendor for resolution, and provide information on user problems to management in order to address systemic problems. Onsite technical support staff should be able to troubleshoot basic hardware, software and application problems. Organizing and implementing frontline technical support should be a priority for Customs.

3.11.1. Ensuring Technical Support for Customs Software

Technical support can be purchased for major software, such as database management systems. This support, however, is often very expensive—in some cases, up to twenty percent of the original cost of the software for one year's worth of support. Customs will need to look very closely at technical support agreements to ensure they are worth the extra cost. For some of the more expensive software, technical support means simply free access to the software firm's helpdesk. The people assisting the customer, however, may or may not be able to resolve the problem, and there are no guarantees according to standard software licenses. In addition, some technical support agreements include free software upgrades. This can save a substantial amount of money if the agreement happens to be in force at the time of a major upgrade. The question still remains, though, if it is worth the expense.

Migrating when there are major version changes of software requires significant planning, and it may be determined that the free upgrades obtained under technical support agreements should not be implemented. Overall, experience on other projects indicates that the Internet is really the best source of information for resolving software problems, and the technical support fees are not worth the expense.

Technical support is also needed for standard software, such as Windows and Microsoft Office. This support can and should be managed internally. Generally, outsourcing this type of technical support is not worth the expense. It should only be seriously considered if the whole IT technical support function is going to be outsourced. Again, the key point is properly training IT staff to provide this support.

Customs applications as a group cover the main Customs Commission Automated System and the other operational systems, such as the human resources and accounting systems. Users need technical support for these applications to answer their questions on system functionality (how to use the system) and to address any system failures or errors. Technical support for these applications is provided either through support contracts or on an informal basis by colleagues and IT staff.

Formal technical support for the Customs Commission Automated System is not being sufficiently provided. The reason is due primarily to contractual disputes over the years with the vendor. This is a very dire situation. Proper technical support must be provided by the vendor supplying the Customs Commission Automated System, since this is the core system for Customs operations.

Technical support for software is generally provided under maintenance contracts, including the Customs Commission Automated System's database management system and the main network and PC operating systems implemented at Customs. The level of support provided and overall cost for this technical support needs to be reviewed.

3.11.2. Providing a Functional Helpdesk

Helpdesk software is often overlooked when an organization is attempting to modernize. This oversight reduces the probability of successfully implementing new systems. The reason is that the technical problems of users are neither tracked nor properly analyzed, and therefore, not adequately addressed. Without reliable information, technical problems tend to linger, users become discouraged and system implementations are jeopardized. One of the key ways to ensuring a smooth system implementation is to track technical problems and correct them as quickly as possible. All system implementations suffer from technical problems or setbacks, but quick action will minimize the impact and avoid disenfranchisement by users. Many IT projects end up failing because user problems are not adequately addressed, and this situation should be avoided by Egyptian Customs. Regardless of the approach taken to upgrading Customs systems (that is, build, buy or outsource), Customs needs to make sure helpdesk software is being used to track and properly address user technical problems.

Currently, no helpdesk software has been implemented by Customs. This is a serious deficiency that needs to be addressed. Customs needs to track problems that users are having with computer systems in order to have them resolved quickly and efficiently. Otherwise, problems that could have been resolved are likely to continue and unnecessarily waste the time of users. Thus, enterprise class network monitoring and helpdesk / trouble ticketing tools should be employed. Some examples to be further investigated for meeting Customs requirements include BMC Patrol for Windows, HP OpenView, IBM Tivoli, and LANDesk Server Manager.

3.12. Establishing and Maintaining IT Governance, Planning, and Support Services

IT planning and support services are neither provided nor managed in a coherent fashion. Numerous players are involved in IT planning, including MoF advisors, donors, the Ministry of Communications, the Customs Reform Unit, as well as the Customs IT managers. This is a very difficult situation to manage effectively. Even though the MoF advisors help coordinate IT projects, more detailed planning is still required to ensure the best return on IT investments—which partially explains why an IT Planning and Support Services Department has been proposed as part of the Technology Sector. Support services, on the other hand, are managed primarily by Customs IT managers. The main support services tasks include technology asset management, procurement, contract management, liaison with other government agencies, and development of IT policies and procedures. The key issue here is a lack of qualified staff. The Manager of IT Operations at Alexandria and a few key staff at his disposal cannot effectively perform all of the support services required for smooth running IT operations, in addition to their responsibilities for day-to-day operations.

The new organizational structure proposed for Customs in the recent IT Gap Analysis addresses the current lack of coordinated and coherent IT planning and support services. The IT Planning and Support Services Department included in the recently proposed organizational structure would include IT consolidated planning, project management, budget monitoring and control, technology asset management, procurement, contract management, liaison with other government agencies and IT policies and procedures (see Appendix C for the proposed organizational structure of the Customs IT Department). As the demands for IT support grow, Customs will need to plan and manage IT more effectively, and this new department will provide a mechanism to accomplish this.

3.12.1. Establishing and Communicating IT Policies and Procedures

IT policies and procedures have only been superficially developed. Formalizing IT policies and procedures will clarify responsibilities, ensure greater consistency of system implementations, reduce problems experienced by users, improve reliability of systems, minimize inappropriate or unauthorized use of systems, protect systems against security threats and enhance the capability for disaster recovery. Some thought has been put into policies and procedures—for example, data backups are performed and a couple of firewalls have been implemented. However, much more needs to be done to formalize policies and procedures. Good IT policies and procedures are the backbone of sound IT management, and having them in place will help IT staff focus on more complex and important issues.

Customs should start developing IT policies and procedures immediately, since they will help with the overall management of the IT function and will significantly aid any future systems implementations. Below is a list of policies and procedures that need to be developed, roughly in their order of priority.

- 1) Anti-virus
- 2) Data Backup
- 3) System Configuration Control
- 4) Confidentiality Agreements
- 5) Data Access and Control
- 6) IT Procurement and Vendor Management
- 7) Network Management and Monitoring
- 8) Database Administration

- 9) Production Testing
- 10) Disaster Recovery
- 11) Problem Escalation
- 12) Helpdesk and Technical Support
- 13) Internet Usage
- 14) System Auditing

Developing and implementing these policies and procedures will substantially improve the management of the IT function, and end users will also notice an improvement in the quality of IT support they receive.

3.12.2. Establishing Enterprise-wide Internet Access Policies and Controls

According to a questionnaire submitted to the Customs IT Department for the gap analysis, only Alexandria has Internet access, and this is on a pilot basis. Internet access, however, is almost impossible to control in this environment. Any office could set up an informal connection to the Internet, specifically through a dialup or ADSL connection. This poses a significant security risk to Customs IT systems. A policy needs to be established to discourage unauthorized access to the Internet.

Internet access needs to be very carefully managed and controlled. All connections to the Internet must be through properly managed proxy servers and firewalls. This requires standardization of proxy server and firewall software and its configuration management. Through the WAN all proxy server and firewall software can be managed centrally.

Unauthorized connections to the Internet are a very serious security risk and must be prohibited. There are numerous ways for informal connections to be made—the easiest of which are dial up and ADSL access. Internet policies should strictly prohibit accessing the Internet through unauthorized Internet services. The main vulnerabilities are from spyware, hackers and viruses. The Customs network needs to be centrally managed and monitored for unauthorized Internet access.

3.13. Instituting Enterprise-wide Antivirus Software

No antivirus software has been implemented by Customs. This is a critical issue that must be addressed as soon as possible. Viruses, trojan horses, worms, spyware and adware can infect Customs computer systems and cause considerable damage—including deleting and erasing data on hard drives. While the design of Microsoft Windows makes it more vulnerable than either Linux or Unix and it is also a favorite target of hackers and virus writers, Customs still needs antivirus software to protect systems running on UNIX and Linux. In addition PCs running on Windows are obviously vulnerable. Customs needs to address this issue as soon as possible and implement a comprehensive antivirus solution.

Implementing antivirus software in Customs is an absolute priority. This deficiency could easily crash the Customs Commission Automated System and other systems, if any kind of malicious code ended up in the network. Antivirus software must be installed on all computers attached to the Customs networks. This comprises at least 900 computers if it is assumed that all of the computers from the two large procurements are connected to the network. Since additional computers have been purchased on an ad hoc basis, the number of PCs connected is almost surely more than 900. In order to resolve this problem, Customs needs to make sure that only computers with licensed software are connected to the Internet, operating system software is regularly updated and enterprise antivirus software is implemented. Enterprise antivirus software will automatically update virus definitions on

computers connected to the network and schedule virus scans. A tender has been prepared for procuring antivirus software, but it is unclear if there is enough funding for all network nodes.

4. OTHER CONSIDERATIONS

4.1. Incorporating Risk Management

A Customs Risk Management Department has been created. This unit, however, is in its very early stages of development, and only two staff members (the planned number of staff is 12) have been assigned to it. These staff members only have standard PCs at this time.

The main IT requirements will be a data analysis server, PCs, and econometrics and data mining software. (It should be highlighted as well that the Risk Management Department will be a user of the planned data warehouse when it is implemented.) TAPR-II recommends SPSS (Statistical Package for the Social Sciences) for the econometrics and data mining software. The table below estimates IT requirements based on a staff of twelve.

4.1.1. Applying Statistical Risk Models

Customs has not created any statistical models yet for risk assessment. This is a high priority, and a project has been funded by the EU TEP-C project to create among other things a risk analysis database and initial risk models.

The Risk Management Department will be tasked with identifying risk criteria that will be fed into the Customs information system to automate selection of shipments for inspection. Since Customs does not have any experience with automated risk management, the EU TEP-C project, through a selected vendor, will provide technical assistance to build the initial risk analysis database and statistical risk models. The risk models will be used to determine the appropriate criteria and weightings for risk selection.

4.2. Maintaining an IT Equipment Inventory

No database system is currently used to manage IT equipment inventory. Implementing such a system would be very helpful for IT planning, tracking equipment warranties and repairs, and procurement activities. An IT equipment inventory database needs to be implemented with standard management reports. Managing this database should be part of the technical support function.

4.3. Managing Software Licensing

Software licenses need to be acquired for all software operating systems within Customs. In particular, special attention should be paid to the Microsoft PC operating systems and office productivity tools, since these are favorite targets of hackers. Customs should be able to avail itself of the Egyptian Government's blanket agreement with Microsoft to obtain proper licenses for these software productions.

Software licensing is another important issue because unlicensed software (besides usually being buggy) poses a serious security threat. Unlicensed software is difficult to update, and if there is a security issue, Customs may not be able to install the appropriate security update necessary to fix the problem, leaving computers with unlicensed software vulnerable to security threats. Customs has numerous machines running unlicensed software. Typically, these machines were ad hoc purchases. Only computers with properly licensed and updated software should be connected to the Customs network. Customs needs to address the issue of software licensing immediately.

Software licenses need to be acquired for all software operating systems within Customs. In particular, special attention should be paid to the Microsoft PC operating systems and office productivity tools, since these are favorite targets of hackers. Customs should be able to avail itself of the Egyptian Government's blanket agreement with Microsoft to obtain proper licenses for these software productions.

4.4. Managing Office Productivity Tools

Most Customs administrative staff need basic office productivity tools. Office productivity tools include software, such as MS Word, Excel, PowerPoint and Outlook. These types of tools are currently used by the small number of administrative staff that have computers. These computers, however, were typically purchased on an ad hoc basis and do not have licensed versions of the software. Licensed versions of office productivity software need to be acquired because unlicensed software is a security risk. Additional licenses will also need to be purchased as more computers are purchased for administrative staff.

4.4.1. Establishing and Managing Customs E-mail

Customs has installed an e-mail server and setup e-mail accounts for about 300 staff—primarily managers. This situation is not surprising. E-mail would not have been a high priority, and it also places significant demands on networks. Consequently, many employees are using the free services, such as Yahoo or Hotmail, available over the Internet. As an interim solution, this works. However, e-mail is a very important tool that improves overall organizational efficiency, and accounts should be set up for all professional staff. In addition government organizations need to maintain records of official correspondence using e-mail. The only way to do this is to set up e-mail accounts for professionals involved in official correspondence and make sure that the e-mail server is properly backed up. Customs needs to keep in mind that correspondence using the free services is lost.

Setting up official e-mail accounts for all professional staff should be a high priority for Customs. The main considerations are to restrict attachments and to ensure proper backup of the server. E-mail attachments need to be restricted in order to avoid overwhelming the network. (Analyzing network traffic should allow Customs to determine the size of attachments that can be allowed.) Data backup in general needs to be addressed by Customs, but it is particularly important to have a permanent record of official correspondence, including via e-mail. Technically, data backup is not difficult. The main issues are establishing proper policies and procedures and monitoring that they are followed properly.

Customs should launch e-mail for all professional staff during the modernization phase to improve overall communication and efficiency within Customs and also because it will be an important tool for communicating to employees during the rollout of new Customs systems. Large complex projects, such as the rollout of a new Customs Commission Automated System, often fail during implementation, and one of the key issues is properly communicating expectations to employees—particular users of new systems. Without proper communication, users often do not know what they are supposed to be doing and revert back to old ways of doing things. E-mail will greatly enhance the ability of the system implementation team to communicate directly with users and other key staff involved in system implementation and will improve the overall chances of successful systems implementations.

4.5. Maintaining the Customs Site Physical Environment

4.5.1. Establishing Physical Security

None of the Customs sites visited, including the current main processing site at Alexandria, has established sufficient physical security for the data processing areas and computer access points. There are no badge/card reader systems in place, or some alternative security access mechanisms. In fact, at several sites it was discovered that physical security was casual during working hours, such that workers “knew” the other people who were there. However, after hours many of those sites completely shut down during non-working hours as a way to secure the systems. This is not a good approach for many reasons, not

the least of which is the fact that this does not completely protect the systems from unwanted access and the practice of shutting down – starting up every day is notoriously harsh for servers, databases, etc., and will age the associated hardware more rapidly.

However, there was one forward-thinking site that may be used as a model for physical access control in the near future – the secondary site of Sohkna. This site is in the early stages of implementing a biometric handprint system, and it does not shut down every evening. Sohkna was advanced in many ways compared with all other sites, including its IT support, partially because it is currently better funded due to employing a different private funding business model. Sohkna achieved additional funding through Amiral and being able to charge service fees to Royal.

Physical security should be approached by Customs in the context of existing building conditions, funding and the need to interact with traders in order to facilitate trade. A balance needs to be struck between the goals of trade facilitation, environmental conditions, limited funds and the need for security. Physical security issues that should be addressed immediately include door locks, window bars, smoke detectors, fire extinguishers, security guards and control procedures for moving IT equipment from buildings.

In the main Customs locations these issues should already be addressed or will be addressed during port renovations. Remote locations, however, will need to be upgraded to meet minimum physical security standards. The main processing centers in Cairo and Alexandria will also require special consideration, due to their ultra-secure requirements.

All Customs locations with IT equipment should have at a minimum door locks, window bars (first floor offices), smoke detectors, fire extinguishers, security guards and control procedures for moving IT equipment from buildings. The remote locations are the primary concern, since the major ports tend to be in good physical condition or are being renovated.

For the main processing centers, which are planned in Cairo and Alexandria (and possibly Port Said), the physical security requirements will be much higher. The primary recommendation, in addition to the normal considerations, is to implement an electronic access system and access cards (for door locks). This kind of system will restrict access to the server rooms and will also track who has been in them. Closed circuit cameras should also be considered at these locations.

4.5.2. Managing Environmental Controls

Environment controls are in reasonably good shape and in general are improving. The main issues to consider are air conditioning, electrical systems and physical security. Air conditioning is a critical issue in major computing centers, due to the climate. All the main computing centers have proper air conditioning. Some of the front office locations (for trader input) and remote locations, however, do not have proper air conditioning. The reliability of electrical systems is another important issue. It has been well addressed at the main Customs locations, but is still an issue in remote locations. Last, physical security needs to be improved in most locations. Some improvements are being made with port upgrades, but tighter physical security will be needed in the future—in particular access to main computing centers. Overall, the environment for computers is in reasonably good shape, and in some locations, the situation has improved substantially because of recent upgrades at the locations.

In general environmental controls in Customs locations are in good shape with the exception of remote locations. The subsections below highlight actions that should be taken during the Interim Modernization Phase. When a full-blown system security review is conducted, additional actions will be identified and can be prioritized.

4.5.3. Managing Electrical Systems

Computer equipment requires reliable and stable electrical power to run properly and avoid damaging the equipment. The electrical systems in buildings where computer equipment is used should be evaluated, unless a building has recently been or is soon to be renovated. The main issues to investigate include:

- Power stability,
- Confirmation that all three electrical phases are working properly,
- Appropriate use of circuit breakers,
- Grounding, and
- Quality of wiring.

A professional electrician needs to evaluate these issues. Based on a professional evaluation, appropriate repairs and upgrades can be made.

According to staff interviewed at Customs, the electrical systems in the main Customs locations are in good shape. The electrical systems operate properly, are in a good state of repair and have a backup diesel generator. The only issue noted is that some of these locations are being renovated, which may cause power disruptions.

In lieu of a proper electrical environment, electrical equipment can be used to ensure a reliable power source and/or protect computer equipment. The normal equipment used includes: generators, UPSs and surge protectors, and voltage regulators.

In any locations where a significant amount of new computer equipment is going to be installed, an electrician needs to evaluate the existing electrical system, that is, unless the Customs location has been recently renovated.

4.5.3.1. Managing UPSs

UPSs are needed to protect equipment from power outages and avoid data loss or corruption. Computer equipment needs to be shutdown properly when there is a power failure, and UPSs can either shutdown a computer automatically or give a computer user time to shutdown a computer manually, depending on the type of UPS. Shutting down computers properly prevents data from being lost or corrupted. This is of particular importance for servers, but is also important for PCs. According to the Operational Manager of the IT Department, UPSs in remote locations are old and should be replaced. The Operational Manager of the IT Department estimates that 10 UPSs are needed for the servers at remote Customs locations.

4.5.4. Ensuring Sufficient Site Air Conditioning

Air conditioning is needed to protect computer equipment from extreme heat and also to reduce the amount of dust in an office, which can also damage computer equipment. The main Customs locations are well equipped where the servers are located, but the front offices where traders submit and print declarations are generally in poor shape. New locations will need air conditioning installed, not to mention remote locations that may also need it. The rule of thumb at a minimum should be that all Customs locations with servers should have air conditioning.

Air conditioning units need to be obtained for all main sites, key remote locations, and some front offices for trader submission of documents. A full review of air conditioning requirements should be conducted to determine exactly what is needed.

5. NEXT STEPS

5.1. Main Customs Processing Sites

The current main data processing center in Alexandria is weak on systems security, IT policies and procedures, staffing, and training. Since we will now have two or three duplicate main customs processing sites, an important first step is to get an initial site right, so it can be replicated. The logical choice for this first prototype main site is Alexandria, so it is recommended that the main site reference architecture, technologies, and security measures advocated in this document be instituted initially in Alexandria, perhaps as a first implementation project towards establishing an overall enterprise architecture based upon the reference architectures. Then the lessons learned from doing this for Alexandria can be propagated to the new Cairo MoF site for the next main site, and then possibly Port Said (if chosen to be a main site).

5.1.1. Main Site at the Cairo MoF

There are preliminary plans to implement the main customs data processing center in Cairo at the Ministry of Finance (MoF) complex. However, these plans have not been fully funded. Additional servers, PCs, the LAN, related networking hardware and peripheral devices still need to be procured. Completing this project during the Interim Modernization Phase is a high priority because it takes time to install the hardware, identify or hire staff to run the center, and prepare the site for normal operations. The main computing center needs to be operational by the time a new Customs information system is ready to be installed.

Customs should go ahead with acquiring, setting up and implementing the basic hardware for the Cairo Data Processing Center and upgrading as necessary the Alexandria site as the future backup data processing center. The main issue is not to be overzealous at the early stages. A conservative approach is appropriate because the exact hardware needs will not be apparent until a new Customs information system has been selected. Nonetheless, it is important to install basic infrastructure, recruit staff and establish these centers as soon as possible. These centers need to be well established before the implementation of a new system.

5.1.2. Backup Site in Alexandria

Alexandria is currently the main IT center and does not need any significant upgrade of systems hardware to become the backup data processing center, besides the two IBM eServer xSeries 255 servers (same as Cairo) it has already received. The old servers currently supporting the CCAS will also then be available to support other systems as needed, after the new CIS is centralized in Cairo. However, this site does need significant security upgrades, both physically and for IT.

5.1.3. Disposition of Port Said

As Customs upgrades its overall systems architecture and key computer systems, it is anticipated that there will be a shift to a centralized n-tier architecture for the new core CIS. This implies creating centralized data processing centers in key locations. For Egyptian Customs, one main data processing center at the Cairo MoF and a backup data processing center at Alexandria are probably sufficient, though a third site at Port Said is currently under consideration. Arguably, this is not necessary, but will not hurt either (though will add some overhead in managing a third main site). The disposition for Port Said needs to be determined in the near future, so appropriate planning and procurement can occur.

5.2. Secondary Customs Processing Sites

Similar to the approach for rolling out the main site reference architecture to the relevant sites, we should choose an example prototype secondary site for initial implementation. A good choice for this is the Sohkna site, since it is relatively further along than other secondary sites. Thus, we can achieve this rollout faster at this site than others, learn from it, and then apply this to the implementation of other secondary sites.

6. SUMMARY OF KEY RECOMMENDATIONS

The key recommendations that have been made in this document, by relative priority, are summarized in Table 3 below. Note the following when reviewing this table:

1. Each set of listed recommendations by priority level can potentially make a good starting point for creating the scope and defining projects or subprojects in order to implement the complete customs enterprise architecture solution shown in the reference architectures of Figures 1 and 2. Thus, all or any part of the list of recommendations within a given priority level can become the scope for a request for proposal (RFP) or project plan.
2. The order of recommendations within each priority level indicates rough sub-priorities within that level, such that the set of recommendations within that priority level can be further ordered if desired.
3. These priority levels and the associated lists of recommendations should be periodically reviewed as part of a broader IT Planning and Governance responsibility to ensure these remain consistent with the business priorities of Egyptian Customs.
4. This is by no means a complete list of all recommendations within this document, but it is intended to highlight key high-level recommendations for which there are in most cases supporting detailed recommendations in the other sections of this document that further address the related subject matter of the recommendation.

#	<u>Recommendation</u>	<u>Priority Level</u> <i>1 = Immediate Need</i> <i>2 = By Interim Mod. Phase (6 month – 1 yr.)</i> <i>3 = Long-Term (1 – 2 yrs.)</i> <i>4 = Nice To Have</i>	<u>Description /</u> <u>Comments</u>
1	Establish Enterprise-wide anti-virus software at all sites, starting with the Main sites	1	Enterprise antivirus software must be procured and implemented as soon as possible. An enterprise solution will automatically update virus definitions on computers connected to the network and schedule virus scans.
2	Select the CIS Vendor	1	The new CIS must be based on a scalable n-tier, Web-based architecture and integrate into a SOA environment. Also, the overall CIS solution must include single window (and/or document workflow) capabilities in order to significantly increase the efficiency of customs administrative procedures, especially when it involves interactions between Customs, GOIEC, and other control agencies.
3	Select the DBMS Platform	1	Either Oracle or Microsoft SQL Server (possibly IBM DB2) should be chosen for the new database management system to support the new CIS, as well as for the data warehouse, and adapters for data exchange, reporting, and workflow

			management. Note that this effort also includes the development of a long-term common data model and migration from the current Sybase platform.
4	Determine all Main Customs Processing Sites	1	Will Port Said be a Main customs processing site, in addition to Alexandria and Cairo MoF?
5	Establish the Customs Intranet IPsec VPN at all sites, starting with the Main sites	1	Both Intranet and Extranet IPsec VPNs need to be established for the sites, according to the reference architectures. This will include the MPLS WAN (Intranet), PSTN dial-up and Internet (DSL) broadband (Extranet), as well as a direct fiber GOEIC connection (Extranet).
6	Establish Firewalls and DMZ's at the Alexandria Main site	1	Appropriate firewalls must be installed wherever there is an Internet, MPLS network, or GOEIC connection. Preferably an edge router / hardware firewall should be combined with a software firewall to increase network security. Also demilitarized zones need to be set up for all the sites. This will require the purchase of new edge routers and other security devices as prescribed in the reference architectures.
7	Upgrade the LAN at the Alexandria Main site	1	LANs in all the main Customs locations eventually need to be upgraded to support 100 Mbps data transfer. This will require replacing all hubs in these locations with only fast Ethernet switches. Customs will still want to use old PCs in their LANs that have 10 Mbps network cards, but replacing the hubs with switches will allow these PCs to connect to the network at the highest speed their individual network cards will support without affecting the overall network speed for other connections.
8	Establish new core switches at all sites, starting with the Main sites	1	In the case of the Main sites, the core switch will also include integrated firewall and IPS capabilities as the connection point to the Customs MPLS Intranet WAN.
9	Determine Strategic Technology Platforms, Standards, and Best Practices.	1	There may be some minor variations on these Customs technology standards for good reasons on a case-by-case basis, but it is important to establish the predominant technology platforms, tools, standards, and best practices to guide strategic and consistent RFPs, vendors, and Customs IT skills. One initial decision needed is whether to employ a primarily Microsoft platform or Java / Open Source platform throughout the enterprise. A short strategic list should be

			generated for which all Customs IT decisions either adhere or provide a business case for varying from. The IT Governance and Program Management Office (PMO) functions will own these decisions and their communications and coordination in the future.
10	Establish / Build an effective Customs IT Department staffed with appropriate skills / experience	1	The Customs IT Department should start a major recruiting drive, since it currently only has 17 IT professionals and is estimated to need about 87 for the initial implementation of a new Customs information system.
11	Establish Enterprise-wide cross-organizational IT Governance and PMO capabilities and processes	1	IT Governance and program (cross-project) management is critical to ensuring strategic cross-site and cross-organizational coordination and prioritization of all Customs IT projects.
12	Establish Site Physical Security at all sites, starting with the Main sites	1	A badge or biometric system should be deployed and managed, preferably across all sites (i.e. not a different technology solution, tools, or policies across sites). Thus, the management of this can become centralized for economies of scale and cost.
13	Develop IT Technical Support capabilities for all sites, starting with the Main sites	1	The development of the IT technical support function needs to be emphasized because technical support is crucial during the implementation of new IT systems. Users that are not well supported tend to become frustrated and often do not use IT systems properly.
14	Establish Enterprise-wide Helpdesk / Trouble Ticketing tools / processes	1	Helpdesk software needs to be implemented in order to track user problems and improve the efficiency of technical support.
15	Create and Maintain an IT Equipment Inventory database for all sites, starting with the Main sites.	1	An IT Equipment database with standard management reports needs to be implemented. This will also require assigning this responsibility to a staff member at every site, and creating a process for reporting and consolidating this information.
16	Establish Site File Servers at all sites, starting with	2	

	the Main sites		
17	Build / Upgrade the LAN(s) at the remaining Main site(s), including the Cairo MoF (and possibly Port Said)	2	LANs in all the main Customs locations eventually need to be built or upgraded to support 100 Mbps data transfer. This will require replacing all hubs in existing locations with only fast Ethernet switches. Customs may still want to use old PCs in their LANs that have 10 Mbps network cards at these existing sites, but replacing the hubs with switches will allow these PCs to connect to the network at the highest speed their individual network cards will support without affecting the overall network speed for other connections. In the case of the Cairo MoF Main site, this network should have no legacy network components and can be built properly from the beginning.
18	Establish Network Domains at the Alexandria Main Site	2	Network domains need to be set up, and users need to be assigned logins and passwords. The main issue to overcome in order to create network domains is the shortage of qualified IT staff to setup network accounts.
19	Establish Firewalls and DMZ's at the Cairo MoF (and Port Said if chosen) Main site(s)	2	Appropriate firewalls must be installed wherever there is an Internet, MPLS network, or GOEIC connection. Preferably an edge router / hardware firewall should be combined with a software firewall to increase network security. Also demilitarized zones need to be set up for all the sites. This will require the purchase of new edge routers and other security devices as prescribed in the reference architectures.
20	Establish Network-based Intrusion Protection System (NIPS) at the Alexandria Main site	2	Network Intrusion Prevention Software (NIPS) should be implemented immediately, and selected Host-based IPS's should be implemented as the relevant servers are to be brought on-line in accordance with the reference architecture.
21	Establish Network Domains at the Cairo MoF (and possibly the Port Said) Main site(s)	2	Network domains need to be set up, and users need to be assigned logins and passwords. The main issue to overcome in order to create network domains is the shortage of qualified IT staff to setup network accounts.
22	Establish Network-based Intrusion Protection System (NIPS) at the Cairo MoF (and possibly Port	2	Network Intrusion Prevention Software (NIPS) should be implemented, and selected Host-based IPS's should be implemented as the relevant servers are to be brought on-line in accordance with the reference architecture.

	Said) Main site(s)		
23	Establish Enterprise-wide E-mail capabilities for Customs employees	2	E-mail should be set up for all administrative and IT employees of Egyptian Customs. Particular emphasis should be placed on system users and IT Support personnel. System users will be of critical importance when rolling out the new CIS, and they need to be fully informed about their roles and responsibilities. A new E-mail server and a backup server will need to be procured. The logical choice for E-mail Server software is Microsoft Exchange Server. Such servers should exist at two or more Main sites to support backup and load balancing capabilities.
24	Re-architect, design, and launch an improved state-of-the-art Customs website	2	The website must be upgraded to meet standard conventions for official government websites. This is planned with EU support.
25	Establish Partially and Fully Secure Web / Portal Services	2	Web and / or Portal Services will be established with the appropriate levels of security for Public and Extranet Users, depending upon the service.
26	Establish Content Management Tools and Processes	2	To support website and web and / or portal services, as well as related document and image management capabilities
27	Establish the Customs Extranet IPsec VPN for the Main sites	2	Both Intranet and Extranet IPsec VPNs need to be established for the sites, according to the reference architectures. This will include the MPLS WAN (Intranet), PSTN dial-up and Internet (DSL) broadband (Extranet), as well as a direct fiber GOEIC connection (Extranet).
28	Implement the new DBMS Platform	2	Either Oracle or Microsoft SQL Server (possibly IBM DB2) should be used for the database management system of the new CIS, as well as for the data warehouse, and adapters for data exchange, reporting, and workflow management. Note that this effort also includes the development of a long-term common data model and migration from the current Sybase platform.
29	Implement the new CIS at all the Main Customs sites	2	Implementation must take into account all the Main Customs sites and ideally launch these in parallel because of the need for synchronization of the processing and data between the sites. However, if they must be rolled out sequentially, extra care must be taken to partition the data so to back up the operational data and launch

			subsequent sites at a synchronization point.
30	Establish Reverse Proxy Servers at all sites, starting with the Main sites	2	
31	Establish the Data Exchange Servers for the Customs Data Interchange (CDI) at all Main sites	2	
32	Establish NIPS at the Secondary sites	2	
33	Establish Workflow Management and a Business Rules Engine for Automated Customs Processing, as well as scheduled and event-driven activities	2	Only at the Main customs processing sites.
34	Establish Enterprise-wide Data Back-up and Disaster Recovery Tools / Processes, starting with the CIS data but including all critical data	2	<p>Customs should obtain a robust data backup and recovery system in order to help meet the goal of 100% uptime of the core CIS, as well as all other critical systems (i.e. including E-mail, Web servers, etc.)</p> <p>Data backup and disaster recovery policies and procedures need to be developed, and compliance with data backup and recovery policies and procedures needs to be regularly audited and periodically tested.</p>
35	Establish New Data Warehouse	2	This will be a reinvention or extension of previous work accomplished to launch a data warehouse; however, this will now utilize the common data model and the same newer DBMS technologies adopted for the CIS operational database.
36	Establish OLAP and Data Reporting capabilities	3	Customs should obtain basic OLAP (and/or report writing) tools in order to generate management reports from the data warehouse that will be built.
37	Further Develop Workflow	4	The Workflow Management capabilities established earlier can be further built out and

	Management Capabilities to include a fully functioning SOA and ESB		configured to encompass broader workflows and rules-driven events with an effective Enterprise Services Bus (ESB).
38	Establish Web / Portal Services at Secondary sites as needed	4	
39	Establish Content Management capabilities at Secondary sites as needed	4	
40	Establish DBMS capabilities at Secondary sites as needed	4	

Table 3. Summary of Key Recommendations by Priority Level

7. EXAMPLE LIST OF PROJECT DELIVERABLES

In pursuing each of these recommendations either as separate projects, or in combinations as projects, the following deliverables should generally be developed (i.e. starting list of deliverables expected from a vendor providing the scope of a project):

1. Project Plan
2. Functional Requirements
3. Technical Requirements
4. High Level Design
5. Detail Design
6. Software Development and Unit Testing
7. Systems Installation and Configuration
8. Systems Integration
9. Systems and Functional Testing
10. Disaster Recovery Plan
11. Deployment Plan
12. User Acceptance Testing
13. Performance Testing and Tuning
14. Solution Launch
15. End User Training and Documentation
16. Systems Support Training and Documentation
17. Warranty Support
18. Maintenance Support

8. VENDOR EVALUATION CRITERIA

Vendor contract awards for projects to implement progressive projects of the prescribed reference architectures as defined in requests for proposal (RFP) will be made to the most advantageous offer based upon the evaluation criteria described below.

8.1. Cost

The cost of hardware, software, systems, and services will be evaluated using the Offer Schedule. Additional capabilities provided in a particular system should be clearly identified.

8.2. Product Specifications

The primary factors affecting overall system performance will be used to evaluate proposed hardware and software / systems (e.g., processor speed, RAM memory, and hard disk space for personal computers).

For all equipment and software / systems, the conformance to the technical specifications and configurations will also be a primary factor. BearingPoint may reject any quotation that offers hardware configurations that greatly exceed the minimum configuration requested and significantly increase the cost. Offeror **MUST** include manufacturer part numbers for **ALL** items. Failure to provide detailed product specifications (including manufacturer and part number) will negatively affect the Offeror's score in this area.

8.3. Strategic Architectural Fit

For all components provided and configured, the Offeror will be evaluated for the solution's strategic fit in the enterprise architecture plans for Egyptian Customs. In particular, the solution should lend itself to the relevant reference architecture introduced in this report, as well as the strategic timing for the introduction of the components.

8.4. Installation, Warranty, Maintenance, and Service

Warranty period, cost of maintenance and service after warranty, availability of local service **MUST** be discussed in detail. Insufficient documentation will negatively affect the Offeror's score in this area. If the Offeror is relying upon manufacturer's depot for service, this fact **MUST** be clearly stated. Maintenance procedures, including contact information and escalation procedures **MUST** be clearly stated. All hardware / software / systems information listed is required to get a positive evaluation for installation, configuration, warranty, maintenance, and service.

8.5. Responsibility and References

An Offeror must be determined to be "responsible". A responsible Offeror has the technical expertise, management capability, workload capacity, and financial resources to perform the work as evidenced for favorable past performance references. Offeror must provide a minimum of three (3) references of past performances that are the same as or similar to the items and services required in this RFP. Offeror must provide financial resources information and references. The information must include names, telephone numbers and emails so that these references can be contacted. Offeror must provide at least three (3)

references for the service provider. Lack of this information will result in rejection of the response.

8.6. Delivery

Preference will be given to vendors that will deliver the equipment /software / systems in **one shipment** and guarantee **30-day** delivery to a designated location after issuance and Offeror's acceptance of the purchase order. Offeror must state a realistic time and number of shipments to deliver all items.

Technical Assistance for Policy Reform II
BearingPoint, Inc,
8 El Sad El Aali Street, 18th Floor,
Dokki, Giza
Egypt
Country Code: 12311
Phone: +2 02 335 5507
Fax: +2 02 337 7684
Web address: www.usaideconomic.org.eg