

DELIVERY ORDER DR-33-06-317
TASK ORDER 37

LISTED/LOW SYSTEMS C&A: Technical Library Voyager Integrated Library System

1.0 OBJECTIVE

The Contractor shall support the OIS in certification and accreditation of a listed information system such that NRC is in compliance and maintains certification and accreditation currency with NIST and FISMA Guidance. The Contractor shall at a minimum develop associated certification and accreditation documentation consistent with the security support task referenced in SOW ENCLOSURE 6 of Delivery Order DR-33-06-317, entitled, "C&A PROCESS AND DELIVERABLES" such that an Authorization to Operate (ATO) which confers full accreditation shall be granted the system. The Contractor shall perform these security support tasks specified for a MODERATE security baseline system.

The Contractor shall develop, at a minimum, the following information system security certification documentation: an E-authentication risk assessment, a security categorization, a risk assessment and a systems security plan.

2.0 SCOPE OF WORK

The Contractor shall provide security analyst staff and develop all requisite systems certification and accreditation documentation such that the Voyager Integrated Library (ILS) obtains an Authorization to Operate (ATO).

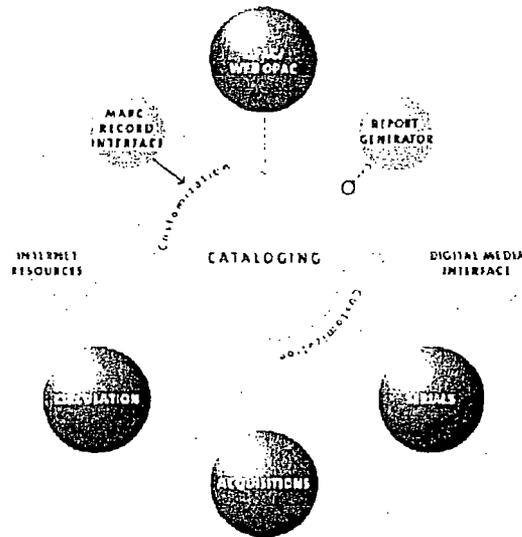
System Name: Voyager Integrated Library System (ILS)

Sponsor Office: Office of Information Services (OIS)

System Owner: Ed Baker, Director, OIS

System Description: Voyager is an integrated library system (ILS) developed by ExLibris Group. It is a commercial off-the-shelf (COTS) "product" and not an in-house system developed for NRC. The ILS is a software package used to perform the primary daily functions required for smooth and efficient library operations. The COTS software provides an automated approach to: cataloging new books and materials, circulation of items, serials management (checking in and routing journals), acquisitions, and searching of the online catalog (OPAC) for books, journals, or other materials for or by patrons.

The Voyager integrated library system (ILS) is a modular system. The primary module that serves as the centralized part of the system is the cataloging module. The cataloging module contains the bibliographic records (public records) which describe the material held in the library (by fields such as author, title, subject, and contents). The remaining modules of the system (e.g., serials, circulation, acquisitions, and the online catalog or OPAC) link over to the records in the cataloging module. In this way, a patron can pull up a bibliographic record in the online catalog, and see information on the item's circulating status (e.g., checked-out or in library), the order status (on order or received) and what issues have been received (if the item is a serial that is checked in). For a pictorial representation of the integrated system, please see the graphic below



The integrated library system has replaced former, and more manual methods of working in the library. It has replaced searching the holdings of a library by using the card catalog, replaced checking-in journals using a cardex system, replaced using paper check-out slips for circulating materials, and paper methods of ordering books and journals. It has automated all these functions into one system, that neatly integrates all aspects of the work and streamlines the processes required to do so.

Status: The Contractor shall provide security analyst staff to develop all requisite system certification and accreditation documentation such that the Voyager ILS obtains an Authorization to Operate (ATO).

Contractor shall provide a security analyst staff for the development of the associated documentation associated with the security support tasks specified below for unclassified LOW security baseline systems for the system category "Listed System", as specified in SOW ENCLOSURE 6 of Delivery Order DR-33-06-317, entitled, "C&A PROCESS AND DELIVERABLES".

OMB policy guidance requires that a security plan be in place for all sensitive systems. NRC uses the term Listed System to refer to a computerized information system or application that processes sensitive information requiring additional security protections, and that may be important to the operations of an NRC office or region, but is not an MA when viewed from an agency perspective. Most NRC systems rely on the security protections provided by the NRC LAN/WAN GSS. However, NRC offices have developed a number of additional non-major applications that are processing sensitive data such as individual privacy act information, law enforcement sensitive information, sensitive contractual and financial information, and other categories of sensitive information that the sponsor has determined will require additional security protections beyond the basic security provided by the NRC LAN/WAN. For those types of non-major applications that the sponsor has built in additional security protections and controls because of the added sensitivity of the information being processed, such a non-major application shall be categorized as a Listed System.

3.0 PERIOD OF PERFORMANCE

The period of performance of this task order is one year from award date.

4.0 FUNDING

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$79,088.88**.

- (b) The amount presently obligated with respect to this task order is **\$79,088.88**. The Contractor shall not be obligated to incur costs above this ceiling/obligated amount unless and until the Contracting Officer shall increase the amount obligated. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this contract. Any work undertaken by the Contractor in excess of the obligated amount specified above is done so at the Contractor's sole risk.

5.0 TRAVEL

No travel is required.

6.0 SCHEDULE

The Contractor shall provide final draft security documentation and reports for the Voyager ILS consistent with the NRC-approved integrated project plan (Subtask 1). Subtask 1, the integrated security Activity Project Plan shall be delivered within one week of task order award.

7.0 SPECIFIC TASKS

The Contractor shall support the NRC C&A of Voyager ILS as described below:

Subtask 1: Integrated Security Activity Project Plan.

Develop and implement a project plan to ensure completion of the certification and accreditation tasks within the period of performance. The Contractor shall be required to develop and maintain an Integrated Security Activity Project Plan and perform Integrated Activity Scheduling for the program. These deliverables shall be developed at the individual project level (i.e., each system for which a certification and accreditation effort will be undertaken) and aggregate to the program level. The Microsoft Project Plan shall incorporate all tasks and projects such that the individual projects roll up into an Integrated Security project schedule encompassing all NRC security related activities, services, and deliverables. The Microsoft Project Plan shall identify resources for each activity and include the Work Breakdown Structure levels. The project plan will include:

- A Level 5 **Work Breakdown Structure (WBS)**. The WBS shall include a definition of the work to be conducted decomposed into distinct discrete manageable tasks or groups of tasks (work packages) with decisive outputs and specific measurable entry and exit criteria. Each work package shall have a short duration, or can be divided into a series of milestones whose status can be objectively measured. Each work package shall be assigned a start and finish date, a budget value, and can be integrated with higher-level schedules.
- A **schedule and budget** for accomplishing the work identifying what resources are needed and how much effort will be required in what time frame to complete each of the tasks in the WBS. The Contractor shall allocate a portion of the budget for each work package that comprises the WBS, and ensure that the WBS adequately defines all work necessary to meet the requirements for the project.

Subtask 2: E-Authentication Risk Assessment.

The Contractor shall conduct E-Authentication risk assessments and generate an E-Authentication risk assessment report consistent with OMB M04-04, NIST SP 800-30, NIST SP 800-60A, and NIST SP 800-63 as part of the security categorization.

Subtask 3: Security Categorization.

The Contractor shall conduct a security scoping interview to determine the proper system or applications classification and Impact consistent with NRC Management Directive 12.5, OMB Circular A-130, FIPS 199, and NIST Special Publication (SP) Series 800. Systems shall be categorized as Major Application, General Support System, Listed, or Other with a system impact of low, moderate, or high. The Contractor shall develop a systems security scoping report that identifies the system investment, system scope, inter-systems connectivity (diagram intersystem connections, data architecture, mapping, and data element definition and exchange between systems), the information sensitivity levels of data processed within the system, the privacy impact of the system and whether it contains information in identifiable form (IFF), the electronic transactions (Inquire, Create, Delete, and Modify) and requisite authentication level, and electronic records disposition.

Subtask 4: Risk Assessment.

The assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation and are required by the Federal Information System Management Act (FISMA) and OMB Circular A-130, Appendix III. Risk assessments influence the development of the security controls for information systems and generate much of the information needed for the associated system security plans.

The risk assessment shall characterize the information processed by using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories. The risk assessment shall follow NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and include the following:

- Identification of user types and associated roles and responsibilities;
- Identification of risk assessment team members and their associations;
- A description of the risk assessment approach and techniques, where the techniques include documentation review, interviews, observation, and system configuration assessments, security scans and penetration tests;
- A description of the risk scale used, including at a minimum, the potential impact as defined in FIPS 199, and likelihood as defined in NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- A list of potential system vulnerabilities;
- A list of potential threat-sources applicable to the system, including natural, human, and environmental threat-sources;
- A table of vulnerability and threat-source pairs and observations about each;
- Detailed findings for each vulnerability and threat-source pair discussing the possible outcome if the pair is exploited; existing controls to mitigate the pair; the likelihood determination as high, moderate, or low; the impact determination expressed as high, moderate, or low; the overall risk rating based upon the risk scale; and the recommended controls to mitigate the risk; and,
- A summary that includes the number of high, moderate, and low findings and provides a list of prioritized action items based upon the findings.

The risk assessment shall be documented in a report that follows the NRC Template for Risk Assessment Report. The report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The NRC Senior IT Security Officer must approve the final to enable system accreditation.

The Contractor shall track any residual risk in the plan of action and milestones (POA&M). The Contractor shall document the results of the process. This shall include documenting the risk number, a description of each risk, the type of risk (i.e., impacting the confidentiality, integrity, or availability), the level of risk (i.e., low, moderate, or high), the associated controls, and the action(s) required or actually performed to eliminate or minimize each risk. The goal is for NRC and Contractor personnel to remediate all high and moderate security findings, and track the remaining security findings in the POA&M.

Subtask 5: Systems Security Plan (SSP).

The security plan shall be developed in accordance with NIST SP 800-53 Recommended Security Controls for Federal Information Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC IT Security Plan Template. The Contractor shall identify within the SSP the necessary security controls required, citing the security controls that are in place, those that are planned, and those that are not applicable.

Where a system relies upon a control that is provided by another system (e.g. the NRC LAN/WAN), the specific control being relied upon shall be noted along with the name of the system providing that control. The Contractor shall trace the security controls to specific documented guidance, NRC policy (e.g., Management Directives), infrastructure policy or procedures.

The system security plan shall be documented in a report that follows the NRC Template for System Security Plan. The report shall be delivered in draft form and then in pre-system ST&E form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the system security plan after completion of the ST&E test report to reflect validated in-place and planned controls. The NRC SITSO must approve the final to enable system accreditation.