EXHIBIT 7.02
Commonwealth Satisfaction Survey Procedures

	Change Order #	Effective Date

In support of Article 7 of the Agreement, the following Commonwealth Satisfaction Survey will be used by Vendor.

Commonwealth will participate in the process, recommend topics for evaluation, validate the survey instrument's questions, identify individuals to be surveyed, recommend how the survey is administered, and in conjunction with Vendor, review both the raw and aggregate data.

Areas identified for improvement will be immediately communicated by Vendor to Vendor staff.

EXHIBIT 7.02
Commonwealth Satisfaction Survey Procedures

IT Organization Satisfaction Survey

Dear (IT Professional):

Your satisfaction is very important to the Unisys Team. We would appreciate you taking a few minutes to complete this survey and return it to us. Your responses should reflect your experience with the Unisys Team since your last survey. In addition to the specific information requested in the survey, any additional comments you may have are very important to us and may be included in the space provided at the end of the survey. Your scoring and comments will be combined to help the Unisys Team meet your needs and expectations, and to help us improve your level of service

Satisfaction definition	Rating	Importance	Rating
Very Satisfied	5	Critical	5
Satisfied	4	Very Important	4
Neither Satisfied nor Dissatisfied	3	Important	3
Dissatisfied	2	Irrelevant	2
Very Dissatisfied	1	Unimportant	1
No recent experience	NE		

- Please place an X on the number in the "Satisfaction Score" column that best describes your level of satisfaction with each factor.
- Please place an X on the number in the "Importance Scale" column that best reflects how important each factor is to you.
- If you have had no experience with a specific factor, please X the NE (No Experience) box.

Name and Title of Survey Respondent: _____

Agency: _____ **Period of Survey:** _____

Phone Number: _____

Please indicate your level of "Satisfaction" and "Importance" for the following:

	Satisfaction	Importance	NE
1. Your overall relationship with the Unisys Data Center Team.	5 4 3 2 1	5 4 3 2 1	[ ]
Rating Comments (optional): _____			
2. Was the Unisys Team sensitive to your concerns and needs and were they resolved in a timely manner?	5 4 3 2 1	5 4 3 2 1	[ ]
Rating Comments (optional): _____			
3. How would you rate your level of satisfaction with the Unisys Project Management team.	5 4 3 2 1	5 4 3 2 1	[ ]
Rating Comments (optional): _____			

EXHIBIT 7.02
Commonwealth Satisfaction Survey Procedures

	Satisfaction	Importance	NE
4. How would you rate the overall attitude and performance of Unisys Data Center personnel.	5 4 3 2 1	5 4 3 2 1	[ ]
Rating Comments (optional): _____			
5. Would you consider engaging Unisys for other I.T. projects in the future?	5 4 3 2 1	5 4 3 2 1	[ ]
Rating Comments (optional): _____			
6. Was the Project Manager flexible with your needs and requirements on this Project?	5 4 3 2 1	5 4 3 2 1	[ ]
Rating Comments (optional): _____			
7. Would you recommend Unisys Services to others?	5 4 3 2 1	5 4 3 2 1	[ ]
Rating Comments (optional): _____			
8. How do you rate the Unisys Team's ability to conduct themselves as professionals.	5 4 3 2 1	5 4 3 2 1	[ ]
Rating Comments (optional): _____			
9. How would you rate System Availability provided by the Unisys Data Center	5 4 3 2 1	5 4 3 2 1	[ ]
Rating Comments (optional): _____			
10. How would you rate Online Subsystem Availability provided by the Unisys Data Center	5 4 3 2 1	5 4 3 2 1	[ ]
Rating Comments (optional): _____			
11. How would you rate Batch / Production quality and timeliness provided by the Unisys Data Center	5 4 3 2 1	5 4 3 2 1	[ ]
Rating Comments (optional): _____			

EXHIBIT 7.02
Commonwealth Satisfaction Survey Procedures

	Satisfaction	Importance	NE
12. How would you rate Online response time provided by the Unisys Data Center	5 4 3 2 1	5 4 3 2 1	[ ]

Rating Comments (optional): _____

_____

13. How would you rate Unisys Help Desk Performance 5 4 3 2 1 5 4 3 2 1 [ ]

Rating Comments (optional): _____

_____

14. Please characterize the frequency of your personal interaction with the following members of the Unisys Team with an appropriate X mark? Also please rate the importance of these interactions on a scale of 1-5 where 5 is Critical.

Unisys Personnel	N/A	Too Often	Often Enough	Too Seldom	Importance
Management					
Operations					
Technical Support					
Disaster Recovery					
Security					

Rating Comments (optional): _____

_____

15. Please rate the overall value and cost of services related to the Unisys Data Center 5 4 3 2 1 5 4 3 2 1 [ ]
Rating Comments (optional)_____

_____

16. What is the one thing the Unisys Team can do more of to improve your satisfaction?
Answer:

_____

_____

_____

_____

_____

_____

EXHIBIT 7.02
Commonwealth Satisfaction Survey Procedures

17. Please indicate if you would like the survey manager to contact you to discuss this survey.

Answer: Yes No

Comments in general:
Comment (s)

Thank you once again for your time and contribution. Please mail this document to the Unisys Data Center Team via inter-office mail or send an electronic version via email at _____. If you have any questions, call the Unisys Data Center Team at 717-___-____.

EXHIBIT 8.01(CSL)
Commonwealth Service Locations

	Change Order #	Effective Date

Department Print Sites

Department	Department of Transportation
Address1	BIS Print Room, 1st Floor Riverfront Office Center
Address	1101 South Front Street
City	Harrisburg
State	PA
Zip	17104

Department	Department of Labor & Industry
Address1	1700 Labor & Industry Bldg.
Address	
City	Harrisburg
State	PA
Zip	17120

Department	Public School Employees' Retirement System
Address1	4th Floor
Address	5 North 5th Street
City	Harrisburg
State	PA
Zip	17108

EXHIBIT 8.01(CSL)
Commonwealth Service Locations

Department	Public Utility Commission
Address1	104 North Office Building
Address	
City	Harrisburg
State	PA
Zip	17120-3265

Department	Game Commission
Address1	2001 Elmerton Avenue
Address	
City	Harrisburg
State	PA
Zip	17110-9797

Department	Department of Public Welfare
Address1	Willow Oak Building, Room 104, Harrisburg State Hospital
Address	
City	Harrisburg
State	PA
Zip	17105-2675

Department	Department of Revenue
Address1	8th Floor, Strawberry Sq
Address	4th and Walnut St
City	Harrisburg
State	PA
Zip	17128-1100

EXHIBIT 8.01(CSL)
Commonwealth Service Locations

Department	State Civil Service Commission
Address1	3rd Floor, Bowman-Worth Bldg
Address	Strawberry Square Complex
City	Harrisburg
State	PA
Zip	17108-0569

Department	Pennsylvania State Police
Address1	3rd Floor, Department Headquarters
Address	1800 Elmerton Ave.
City	Harrisburg
State	PA
Zip	17110

Department	Department of Aging
Address1	Forum Place
Address	555 Walnut St.
City	Harrisburg
State	PA
Zip	17101-1919

Department	Department of Corrections
Address1	P.O. Box 598
Address	2520 Lisburn Rd.
City	Camp Hill
State	PA
Zip	17001-0598

EXHIBIT 8.01(CSL)
Commonwealth Service Locations

Department	Liquor Control Board
Address1	Northwest Office Building
Address	
City	Harrisburg
State	PA
Zip	17124-0001

Department	Department of State
Address1	3rd Floor, North Office Building
Address	
City	Harrisburg
State	PA
Zip	17110

Department	Department of Insurance
Address1	1326 Strawberry Square
Address	13th Floor
City	Harrisburg
State	PA
Zip	17120

Department	Department of Environmental Protection
Address1	Rachel Carson State Office Building, 400 Market Street
Address	P.O. Box 2063
City	Harrisburg
State	PA
Zip	17105-2063

EXHIBIT 8.01(VSL)
Vendor Service Locations

	Change Order #	Effective Date

Systems will be housed at:

Data PowerHouse
Harrisburg State Hospital
Building 43 (Willow Oak Building)
North Circle Drive
Harrisburg, PA 17105

Unisys Project Office will be at:

Unisys Corporation
Suite 102
3605 Vartan Way
Harrisburg, PA 17110

EXHIBIT 8.02
Security Procedures

	Change Order #	Effective Date

Vendor will provide physical and logical security functions in a manner that meets Commonwealth's requirements.

Data PowerHouse (DPH) Physical Security:

[redacted]

EXHIBIT 8.02
Security Procedures

[redacted]

[redacted]

[redacted]

[redacted]

General Security Guidelines:

[redacted]

[redacted]

[redacted]

EXHIBIT 8.02
Security Procedures

Security and Confidentiality (X Responsible, P – Principal, I – Input)	Responsibility	
	Vendor	Commonwealth
Systems Logical Security		
Define security policies, procedures and standards		X
Assign Vendor Security Officer to work with Commonwealth to coordinate Vendor implementation of Commonwealth's policies and procedures for in-scope functions	X	
Ensure security software installation meets C2 security rating	X	
Collect data, monitor and report upon logical security system loggings	X	
Security administration including definition of userids, handling revoked passwords, granting or denying access to resources that include transactions, disk and tape files, databases, execution of batch jobs and database utilities,		X
Security administration including determining authority and access levels for userids, and resources that include transactions, disk and tape files, databases, execution of batch jobs and database utilities		X
Security administration for custom application level security –internal tables/files/program code		X
Network Security		
For in-scope hardware/connections per Commonwealth policy	X	
Support for Commonwealth encryption software	P	I
Destruction of Sensitive Data		
Adhere to Commonwealth policy on Clearing, Purging, and Destruction of Mass Storage Devices	X	
All residual data must be purged from storage devices prior to maintenance and/or re-use outside of the Data PowerHouse	X	
Scratched and damaged tapes/cartridges are disposed of in accordance with the Commonwealth approved Vendor Disposal Procedures	X	
Shred sensitive paper documents (may involve engaging a vendor who specializes in this service)	X	
Logical and physical security audit		
Conduct annual logical and physical security audit	X	
Establish relationships with and involve law enforcement personnel and PEMA	X	
Prepare and submit Detailed Security Report	X	
Provide Executive Summary Presentation	X	
Determine course of action based upon review	X	X
Develop Security Plan	P	I
Execute Security Plan	P	I
Conduct background checks on new hires	X	

EXHIBIT 8.02
Security Procedures

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized.

EXHIBIT 8.02
Security Procedures

In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

EXHIBIT 8.02
Security Procedures

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

(a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

(1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies....

(6) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

(7) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract.

EXHIBIT 8.02
Security Procedures

If privatized, the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

EXHIBIT 8.02
Security Procedures

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES

SECURITY ADDENDUM

The goal of this document is to provide adequate security for criminal justice systems while under the control or management of a private entity, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security and data security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Administration of criminal justice - the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment.

1.02 Agency Coordinator (AC) - a staff member of the Contracting Government Agency, who manages the agreement between the Contractor and agency.

1.03 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

EXHIBIT 8.02
Security Procedures

1.04 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

1.05 Control Terminal Agency (CTA)- a duly authorized state or federal criminal justice agency with direct access to the National Crime Information Center (NCIC) telecommunications network providing statewide (or equivalent) service to its criminal justice users with respect to the various systems managed by the FBI CJIS Division.

1.06 Control Terminal Officer (CTO)- an individual located within the CTA responsible for the administration of the CJIS network for the CTA.

1.07 Criminal Justice Agency (CJA)- The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

1.08 Noncriminal Justice Agency (NCJA) - a governmental agency or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

1.09 Noncriminal justice purpose - the uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

1.10 Security Addendum - a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations, provides for sanctions, and contains such other provisions as the Attorney General may require.

2.00 Responsibilities of the Contracting Government Agency

2.01 The CGA entering into an agreement with a Contractor is to appoint an AC.

2.02 In instances in which responsibility for a criminal justice system has been delegated by a CJA to a NCJA, which has in turn entered into an agreement with a Contractor, the CJA is to appoint an Agency Liaison to coordinate activities between the CJA and the NCJA and Contractor. The Agency Liaison shall, inter alia, monitor compliance with system security

requirements. In instances in which the NCJA's authority is directly from the CTA, there is no requirement for the appointment of an Agency Liaison.

2.03 The AC will be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of certification testing and all required reports by NCIC.

2.04 The AC has the following responsibilities:

a. Understand the communications and records capabilities and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA;

b. Participate in related meetings and provide input and comments for system improvement;

c. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees;

d. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor;

e. Maintain up-to-date records of employees of the Contractor who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date certified or recertified (if applicable);

f. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for a certification exam with the CTA staff. Schedule new operators for the certification exam within six (6) months of employment. Schedule certified operators for re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for any other mandated class;

g. The AC will not permit an un-certified employee of the Contractor to access an NCIC terminal;

h. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements;

EXHIBIT 8.02
Security Procedures

i. Provide completed Applicant Fingerprint Cards on each person within the Contractor who accesses the System to the CJA (or, where appropriate, CTA) for criminal background investigation prior to such employee accessing the system; and

j. Any other responsibility for the AC promulgated by the FBI.

2.05 The CTA shall ensure that all NCIC hot file transactions and Interstate Identification Index (III) transactions be maintained on an automated log for a minimum of six months. This automated log must identify the operator on III transactions, the agency authorizing the transactions, the requester, and any secondary recipient. This information can be captured at log on and can be a name, badge number, serial number, or other unique number.

3.00 Responsibilities of the Contractor

3.01 The Contractor shall maintain a security program which complies with this Security Addendum.

3.02 The Contractor shall assign a Security Officer accountable for the management of this security program. This person shall coordinate with the CGA to establish the security program.

3.03 The Contractor shall document the security program in a Security Plan. The Security Plan shall describe the implementation of the security requirements described in this Security Addendum, the associated training program, and the reporting guidelines for documenting and communicating security violations to the CGA. The Security Plan shall be subject to the approval of the CJA, even in instances in which the CGA is the NCJA.

3.04 The Contractor shall provide for a Security Training Program for all Contractor personnel engaged in the management, development, operation, and/or maintenance of criminal justice systems and facilities. Annual refresher training shall also be provided.

3.05 The Contractor shall establish a security violation response and reporting procedure to discover, investigate, document, and report on all security violations. Violations which endanger the security or integrity of the criminal justice system or records located therein must be communicated to the CGA immediately. Minor violations shall be reported to the CGA on a periodic basis, but in no instance less than quarterly. See Section 8.01.

3.06 The Contractor's facilities will be subject to unannounced security inspections performed by the CGA. These facilities are also subject to periodic FBI and state audits.

EXHIBIT 8.02
Security Procedures

3.07 The security plan is subject to annual review by the CJA and the Contractor. During this review, provision will be made to update the program in response to security violations, changes in policies and standards, and/or changes in federal and state law and technology.

3.08 The Contractor and its employees will comply with all federal and state laws, rules, procedures and policies formally adopted by the FBI and the CJIS APB, including those governing criminal history record information.

4.00 Site Security

4.01 The Contractor shall dedicate and maintain control of the facilities, or areas of facilities, that support the CGA.

4.02 All terminals physically or logically connected to the computer system accessing NCIC and the criminal justice files must be segregated and screened against unauthorized use or observation.

5.00 System Integrity

5.01 Only employees of the Contractor, employees of CGA, the Agency Liaison, and such other persons as may be granted authorization by the CGA shall be permitted access to the system.

5.02 The Contractor shall maintain appropriate and reasonable quality assurance procedures.

5.03 Access to the system shall be available only for official purposes consistent with the appended Agreement. Any dissemination of NCIC data to authorized employees of the Contractor is to be for their official purposes.

5.04 Information contained in or about the system will not be provided to agencies other than the CGA or another entity which is specifically designated in the contract.

5.05 All criminal history record information requests must be envisioned and authorized by the appended Agreement. A current up-to-date log concerning access and dissemination of criminal history record information shall be maintained at all times by the Contractor.

5.06 The Contractor will ensure that its inquiries of NCIC and any subsequent dissemination conforms with applicable FBI/NCIC policies and regulations, as set forth in the NCIC Operating Manual, NCIC and CJIS APB meeting minutes, and all relevant CJIS security documents. All disseminations will be considered as "Unclassified, For Official Use Only."

EXHIBIT 8.02
Security Procedures

5.07 The Contractor shall protect against any unauthorized persons gaining access to the equipment, any of the data, or the operational documentation for the criminal justice information system. In no event shall copies of messages or criminal history record information be disseminated other than as envisioned and governed by the appended Agreement.

6.00 Personnel Security

6.01 Appropriate background investigations must be conducted on all Contractor employees and the Contractor's vendors which provide system maintenance support.

6.02 Thorough background screening by the CGA is required. This investigation includes submission of a completed applicant fingerprint card to the FBI through the state identification bureau. State and national record checks by fingerprint identification must be conducted for all personnel who manage, operate, develop, access and maintain criminal justice systems and facilities. Record checks must be completed prior to employment.

6.03 When a request is received by the CTA before system access is granted:

a. The CGA on whose behalf the Contractor is retained must check state and national arrest and fugitive files. These checks are to be no less stringent than those performed on CJA personnel with access to NCIC.

b. If a record of any kind is found, the CGA will be formally notified, and system access will be delayed pending review of the criminal history record information. The CGA will in turn notify the Contractor-appointed Security Officer.

c. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA's designee will review the matter. A Contractor employee found to have a criminal record consisting of any felony convictions or of misdemeanor offenses which constitute a general disregard for the law is disqualified. Applicants shall also be disqualified on the basis on confirmations that arrest warrants are outstanding for such applicants.

d. If an adverse employment determination is made, access will be denied and the Contractor-appointed Security Officer will be notified in writing of the access denial. This applicant will not be permitted to work on the contract with the CGA. Disqualified employees and applicants for employment shall be notified of the adverse decisions and the impact that such records had on such decisions.

EXHIBIT 8.02
Security Procedures

6.04 The investigation of the applicant's background shall also include contacting of employers (past or present) and personal references.

6.05 The Security Officer shall maintain a list of personnel who successfully completed the background investigation.

6.06 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes.

6.07 The CGA shall ensure that each Contractor employee authorized to access CJIS network terminals or information provided therefrom is specially trained in the state and federal laws and rules governing the security and integrity of criminal justice information.

6.08 All visitors to sensitive areas of Contractor facilities must be escorted at all times by a Contractor employee with clearance. Names of all visitors shall be recorded in a visitor log, to include date and time of visit, name of visitor, purpose of visit, name of person visiting, and date and time of departure. The visitor logs shall be maintained for five years following the termination of the contract.

7.00 System Security

7.01 Transmission, processing, and storage of CJA information shall be conducted on dedicated systems. Increased reliance should be placed on technical measures to support the ability to identify and account for all activities on a system and to preserve system integrity.

7.02 The system shall include the following technical security measures:

a. unique identification and authentication for all interactive sessions;

b. if warranted by the nature of the contract, advanced authentication techniques in the form of digital signatures and certificates, biometric or encryption for remote communications;

c. security audit capability for interactive sessions and transaction based logging for message-based sessions; this audit shall be enabled at the system and application level;

d. access control mechanisms to enable access to be restricted by object (e.g., data set, volumes, files, records) to include the ability to read, write, or delete the objects;

e. ORI identification and access control restrictions for message based access;

f. system and data integrity controls;

g. access controls on communications devices;

h. confidentiality controls (e.g., partitioned drives, encryption, and object reuse).

7.03 Data encryption shall be required throughout the network passing through a shared public carrier network.

7.04 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

7.05 The Contractor shall establish a procedure for sanitizing all fixed storage media (e.g., disks, drives) at the completion of the contract and/or before it is returned for maintenance, disposal or reuse. Sanitization procedures include overwriting the media and/or degaussing the media. If media cannot be successfully sanitized it must be returned to the CGA or destroyed.

8.00 Security violations

8.01 Consistent with Section 3.05, the Contractor agrees to inform the CGA of system violations. The Contractor further agrees to immediately remove any employee from assignments covered by this contract for security violations pending investigation. Any violation of system discipline or operational policies related to system discipline are grounds for termination, which shall be immediately reported to the AC in writing.

8.02 The CGA must report security violations to the CTO and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

8.03 Security violations can justify termination of the appended agreement.

8.04 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including the actual NCIC telecommunications link. The FBI will provide the CTO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CJA and Contractor. Upon termination, the Contractor's records containing criminal history record information must be deleted or returned to the CGA.

8.05 The FBI reserves the right to audit the Contractor's operations and procedures at scheduled or unscheduled times. The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

9.00 Miscellaneous provisions

9.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CTA, and FBI.

9.02 The following documents are incorporated by reference and made part of this agreement: (a) The III, NCIC, and Uniform Crime Reporting Operating Manuals; (b) The Minutes of the CJIS APB; (c) The Bylaws for the CJIS APB and CJIS Working Groups; (d) Title 28, Code of Federal Regulations, Part 20; (e) The NCIC Security Policy (including all concepts of NCIC Computerized Criminal History Program Background, Concept and Policy); (f) The Recommended Voluntary Standards for Improving the Quality of Criminal History Record Information, NCIC Standards, and UCR Standards, as recommended by the CJIS APB; and (g) Applicable federal and state laws and regulations.

9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

9.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

9.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

EXHIBIT 8.02
Security Procedures

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I have read and am familiar with the contents of this Security Addendum, including relevant portions of the underlying documents, including but not limited to the III, NCIC, and UCR Operating Manuals; relevant Minutes of the CJIS Advisory Policy Board; Bylaws for the CJIS Advisory Board and CJIS Working Groups; Title 28, Code of Federal Regulations, Part 20; NCIC Security Policy; Recommended Voluntary Standards For Improving the Quality and Criminal History Record Information; NCIC and UCR Standards; as well as applicable federal or state laws and regulations regarding dissemination of criminal history records for criminal and noncriminal justice purposes.

_____
Signature of Contractor Representative

_____ _____
Organization and Title Date

I acknowledge that I have read this Security Addendum and understand its contents.

_____ _____
Signature of Contractor Employee Date

EXHIBIT 8.02
Security Procedures

COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE AGREEMENT

Health Insurance Portability and Accountability Act (HIPAA) Compliance

WHEREAS, the Commonwealth of Pennsylvania as a hybrid entity (Covered Entity) and Unisys Corporation (Business Associate), intend to protect the privacy and provide for the security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the HIPAA Privacy Rule (Privacy Rule) modifying 45 CFR Parts 160 and 164, and the HIPAA Security Rule (Security Rule), modifying 45 CFR Parts 160, 162 and 164.

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI can be used or disclosed only in accordance with the Outsourcing Agreement (ME 981363), any amendments thereto ("the Agreement"), and the standards established by HIPAA and the Privacy Rule.

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, that is in electronic form, which PHI must be handled in accordance with the Agreement and the standards established by HIPAA and the Security Rule, beginning as soon as practicable but in no event later than the effective date of the Security Rule.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1. **Definitions.**
   a. "Business Associate" shall have the meaning given to such term under the Privacy and Security Rules, including but not limited to, 45 CFR §160.103.
   b. "Covered Entity" shall have the meaning given to such term under the Privacy and Security Rules, including, but not limited to, 45 CFR §160.103.
   c. "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
   d. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164.
   e. "Protected Health Information" or "PHI" means any information, transmitted or recorded in any form or medium; (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations at 45 CFR Parts 160, 162 and 164, including, but not limited to 45 CFR §164.501.
   f. "Security Rule" shall mean the Security Standards at 45 CFR Parts 160, 162 and 164.
   g. Terms used, but not otherwise defined, in this Appendix shall have the same meaning as those terms in 45 CFR Parts 160, 162 and 164.

2. **Stated Purposes For Which Business Associate May Use Or Disclose PHI.** Except as otherwise limited in the Agreement, Business Associate shall be permitted to use or disclose PHI provided by or obtained on behalf of Covered Entity to perform those functions, activities, or services for, or on behalf of, Covered Entity which are specified in this contract's Appendix A (Statement of Work), provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

EXHIBIT 8.02
Security Procedures

3. **Additional Purposes For Which Business Associate May Use Or Disclose Information.** In addition to the Stated Purposes, Business Associate may use or disclose PHI provided by, or created or obtained on behalf of Covered Entity for the following additional purposes:

   a) **Use Of Information For Management, Administration And Legal Responsibilities.** Business Associate is permitted to use PHI if necessary for the proper management and administration of Business Associate or to carry out legal responsibilities of the Business Associate except as otherwise limited in the Agreement.

   b) **Disclosure Of Information For Management, Administration And Legal Responsibilities.** Business Associate is permitted to disclose PHI provided by, or created or obtained on behalf of Covered Entity for the proper management and administration of Business Associate or to carry out legal responsibilities of Business Associate, except as otherwise limited in the Agreement, provided:

      i) The disclosure is Required By Law: or
      ii) The Business Associate obtains reasonable assurances in writing from any third party to whom the information is disclosed that it will be held confidentially and used or further disclosed only as Required By Law or for the purposes for which it was disclosed to the third party, the third party will use appropriate safeguards to prevent other use or disclosure of the information, and the third party agrees to immediately notify the Business Associate of any instance of which it is aware in which the confidentiality of the information has been breached.

   c) **Data Aggregation Services.** Business Associate may also be permitted to use PHI to provide data aggregation services, as that term is defined by 45 CFR §164.501. 45 CFR §164.504(e)(2)(i)(B).

   d) Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1).

4. **BUSINESS ASSOCIATE OBLIGATIONS:**

   a) **Limits On Use And Further Disclosure Established By This Appendix And Law.** Business Associate hereby agrees that the PHI provided by, or created or obtained on behalf of Covered Entity shall not be further used or disclosed other than as permitted or required by this Appendix or as Required By Law.

   b) **Appropriate Safeguards.** Beginning as soon as practicable but in no event later than the effective date of the Security Rule, Business Associate shall use appropriate administrative, physical and technical safeguards designed to prevent any use or disclosure of PHI other than as provided for by this Appendix. For purposes of this Appendix, "appropriate safeguards" may include those that are (i) consistent with Business Associate's business practices and are; (ii) no less protective than Covered Entity's instructions as mutually agreed to in this Agreement ME-_981363 and its subsequent alterations and change orders. Administrative safeguards shall include a system of sanctions for any employee, subcontractor or agent who violates this Appendix or the Privacy Rule. 45 CFR §164.504(e)(2)(ii)(B); 45 CFR §164.314(a)(1)(i) and 45 CFR §164.314(a)(2)(i)(A).

EXHIBIT 8.02
Security Procedures

c) **Reports Of Improper Use Or Disclosure.** Business Associate hereby agrees that it shall report within five (5) business days to the Covered Entity Program Administrator any use or disclosure of PHI not provided for or allowed by this Appendix of which it becomes aware. 45 CFR §164.504(e)(2)(ii)(C).

d) **Reports Of Security Incidents.** Beginning as soon as practicable but in no event later than the effective date of the Security Rule, Business Associate hereby agrees that it shall report within five (5) business days to the Covered Entity Program Administrator any security incident of which it becomes aware. 45 CFR §164.314(a)(2)(i)(C).

e) **Subcontractors And Agents.** Business Associate hereby agrees that any time PHI is provided or made available to any subcontractors or agents, Business Associate agrees to ensure that such contractors and agents agree to the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Appendix. 45 CFR §164.504(e)(2)(i)(B).

f) **Right Of Access To PHI.** Business Associate hereby agrees to allow an individual who is the subject of PHI maintained in a designated record set, to have access to and inspect or copy that individual's PHI. Business Associate shall provide PHI in the format requested, unless it cannot readily be produced in such format, in which case it shall be provided in standard hard copy. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity of same within five (5) business days. Business Associate shall conform to and meet all of the requirements of 45 CFR §164.524.

g) **Amendment And Incorporation Of Amendments.** Within thirty (30) days of receiving a request from Covered Entity for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available and incorporate the amendment to enable Covered Entity to comply with 45 CFR §164.526. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity of same within five (5) business days.

h) **Provide Accounting Of Disclosures.** Business Associate agrees to maintain a record of all disclosures of PHI in accordance with 45 CFR §164.528. Such records shall include, for each disclosure, the date of the disclosure, the name and address (if known) of the recipient of the PHI, a description of the PHI disclosed, the purpose of the disclosure, and shall include disclosures made on or after the date which is six (6) years prior to the request or April 14, 2003, whichever is later. Business Associate shall make such record available to the Covered Entity in a time and manner prescribed by the Privacy Rule and shall provide a copy of the record to the Covered Entity.

i) **Access To Books And Records.** Business Associate hereby agrees to make its internal practices, books, and records relating to the use or disclosure of PHI received from, or created or received by Business Associate on behalf of the Covered Entity, available to the Secretary of Health and Human Services or designee for purposes of determining Covered Entity's compliance with the HIPAA Privacy Regulations.

j) **Maintenance of PHI.** Notwithstanding section 6 of this Appendix, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under section 4(h) of this Appendix for a period of six (6) years after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.

k) **Mitigation Procedures.** Business Associate agrees to mitigate, to the maximum extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Appendix or the Privacy Rule. 45 CFR §164.530(f).

l) **Failure to Perform Obligations.** In the event Business Associate fails to perform its obligations under this Appendix, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Appendix and applicable law.

m. **Property Rights.** The PHI shall be and remain the property of Covered Entity or any Business Associates in privity with the Covered Entity that provides PHI to Business Associate. Business Associate agrees that it acquires no title or rights to the PHI except to the extent provided by law.

5. **OBLIGATIONS OF COVERED ENTITY:**

a) **Provision of Notice of Privacy Practices.** Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with 45 CFR §164.520, as well as changes to such notice.

b) **Permissions.** Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware, if such changes affect Business Associate's permitted or required uses and disclosures.

c) **Restrictions.** Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

d) **Notification of Limitations.** Covered Entity shall notify Business Associate of any limitation(s) in the Notice of Privacy Practices of Covered Entity in accordance with 45 CFR §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

e) **Use or Disclosure of PHI.** Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity.

6. **TERMINATION:**

a) **Termination for Breach.** The Covered Entity may, by written notice of default to Business Associate, terminate the Agreement in whole or in part in accordance with Section 28.03 of the Agreement if the Covered Entity determines that Business Associate has breached a material term of this Appendix.

b) **Effect of Termination.** Upon termination of the Agreement, Business Associate will return or destroy all PHI created or obtained on behalf of the Covered Entity that Business Associate still maintains and retain no copies of PHI; provided that if such

return or destruction is not feasible, Business Associate will extend the protections of this Appendix to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. If Business Associate elects to destroy PHI, Business Associate shall notify Covered Entity. The obligations of this section shall survive termination of this Agreement. 45 CFR § 164.504(e)(2)(ii)(I).

7. **MISCELLANEOUS:**

a) **Regulatory References.** A reference in this Appendix to a section in the Privacy or Security Rules means the section as in effect or as amended as reasonably determined by the Covered Entity.

b) **Amendment.** The Parties agree to take such action as is necessary to amend this Appendix from time to time as is necessary for the Covered Entity to comply with the requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

c) **Survival.** The respective rights and obligations of Business Associate under section 4(j) of this Appendix shall survive the termination of the Agreement.

d) **Interpretation.** Any ambiguity in this Appendix shall be resolved to permit Covered Entity to comply with the Privacy and Security Rules as reasonably determined by the Covered Entity.