List of NIST Requirements met by HBSS ITMS 7.0 Platform

ID	Product Questionnaire	Response	Comments (e.g., N/A)	Policy/Standard Reference
P.1	Does the product support the creation of unique user identifiers and associated authentication features that can be integrated using lightweight access directory protocol and secure lightweight directory access protocol? If not able to integrate into an existing directory access protocol, does the product support creation of user accounts through a system that allows for audit of user creation, modification, disabling, and termination actions	ITMS 7.0 user account management module comes with a built-in LDAP/Secure LDAP integration and is fully compliant with this requirement.		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.2	Does the product allow configuration of access control groups for unique user identifiers?	Yes, via its configurable role management module.		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.3	Is the product capable of demonstrating approval of unique user identifiers by an authorizing party (e.g., super user/administrator)?	Yes		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.4	Does the product support access restrictions based on group assignments including unique identifiers or groups which can read, write and execute files, commands or code associated with commands?	In ITMS 7.0 the data is stored primarily in database and not in files. The user restrictions are managed via user role module and meets this requirement.		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.5	Does the product allow unique user identifiers to be activated, deactivated, and/or deleted?	Yes, via the LDAP interface.		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.6	Does the product support the ability to automatically disable access based on a preset period-of-time established by the Agency?	Yes		NIST SP 800-53 Access Control Moderate Baseline Requirement

P.7	Does the product support audit logging and email notification in the event of account creation, modification, disabling and termination actions?	Yes		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.8	Does the product support automatic logout in the event of inactivity from unique user identifiers?	Yes, this capability is required by HIPAA for external access via browsers, and can be configured for the customer.		NIST SP 800-53 Access Control Moderate Baseline Requirement

P.9	Does the product allow monitoring and reporting (e.g., email) of system account usage?	Yes		NIST SP 800-53 Access Control High Baseline Requirement
P.10	Does the product support automated alerts in the event that a unique user identifier or system account is used outside of a preset period of time as determined by Transit Authority?	Yes		NIST SP 800-53 Access Control High Baseline Requirement
P.11	Does the product allow reporting on atypical usage of unique user identifier or system accounts via electronic mail.	Yes		NIST SP 800-53 Access Control High Baseline Requirement
P.12	Does the product support reporting on user privileges via electronic mail?	Yes		NIST SP 800-53 Access Control High Baseline Requirement
P.13	Is the product capable of tracking and monitoring the assignment of privileged roles (privileged roles are defined as unique user identifiers or system accounts with read, write and execute permissions) via electronic mail?	Yes		NIST SP 800-53 Access Control High Baseline Requirement
P.14	Does the product support the ability to restrict access to it by Internet Protocol Address?	Yes		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.15	Does the product support assignment of discretionary or mandatory access control?	Yes		NIST SP 800-53 Access Control Control Enhancement
P.16	Does the product support the ability to restrict information flow control on metadata?	Yes		NIST SP 800-53 Access Control Control Enhancement
P.17	Is the product capable preventing encrypted data from bypassing content-checking mechanisms?	Yes		NIST SP 800-53 Access Control Control Enhancement
P.18	Does the product allow configuration of unique user identifiers and system accounts with different access permissions separating key functions based on user or group (i.e., separation of duties).	Yes, via ITMS User role management module		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.19	Is the product capable of restricting access based on role or group (e.g., group account policy)?	Yes, via ITMS User Role Management module		NIST SP 800-53 Access Control Moderate Baseline Requirement

P.20	Is the product capable of logging unsuccessful logon attempts and automatically disabling unique user identifiers or system accounts based on a present number of unsuccessful attempts as defined by Transit Authority?	Yes		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.21	Does the product support configuration of a logon banner prior to permitting access that has content defined by Transit Authority?	Yes		NIST SP 800-53 Access Control Moderate Baseline Requirement

P.22	Does the product support logging of last successful and unsuccessful logon attempt for unique identifiers?	Yes		NIST SP 800-53 Access Control Elected Control
P.23	Is the product capable of restricting the number of sessions that are allowed to itself as defined by Transit Authority?	Yes		NIST SP 800-53 Access Control Elected Control
P.24	Is the product capable of locking a session automatically after a preset period of time as defined by Transit Authority?	Yes		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.25	Is the product capable of requiring all transactions have an associated unique user identifier or system account prior to transaction initiation?	Yes		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.26	Is the product capable of tagging information with access permission rights, so that the information can only be viewed with proper credentials regardless of where it is stored?	Yes during initial product configuration and subsequent		NIST SP 800-53 Access Control Elected Control
P.27	Is the product capable of restricting remote access except through approved Transit Authority mediums such as the Virtual Private Networking (VPN) infrastructure?	Yes		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.28	Is the product capable of restricting wireless access except through approved Transit Authority wireless solutions?	Yes		NIST SP 800-53 Access Control Moderate Baseline Requirement
P.29	Is the product capable restricting unique user identifiers' access to other unique user identifiers' information, directory structure, etc. unless otherwise permitted by a user with super user/administrative access?	Data is shared between all users and as such data		NIST SP 800-53 Access Control Moderate Baseline Requirement

		access can only be restricted via role restrictions. HICS is used for information sharing among users, and that can be used to restrict access of one user to data of another user. File systems can be managed by the client.		
P.30	Is the product capable of logging and recording all unique user identifier activity and system account activity?	ITMS 7.0 logs all session activity, and records all data entry and updates done by users.		NIST SP 800-53 Audit and Accountability Moderate Baseline Requirement
P.31	Is the product capable of logging and recording all changes which occur on the asset including applications, databases, network or system operating systems?	ITMS 7.0 maintains a change log to record all changes to assets.		NIST SP 800-53 Audit and Accountability Elected Control
P.32	Is the product capable of logging system and activity transactions including date, time and whether the event was successful?	Yes		NIST SP 800-53 Audit and Accountability Moderate Baseline Requirement
P.33	Is the product capable of storing log data on a predefined amount of storage as defined by Transit Authority?	Yes		NIST SP 800-53 Audit and Accountability Moderate Baseline Requirement

P.34	Is the product capable of alerting via email if log data is not successfully recorded? If not, is there another facility for alerting of errors in logging	Yes		NIST SP 800-53 Audit and Accountability Elected Control
P.35	Is the product capable of recording software / hardware errors and when storage capacity has been reached?	Yes		NIST SP 800-53 Audit and Accountability
				Elected Control
P.36	Is the product capable of logging messages using the "syslog" or "syslog-ng" protocol in compliance with RFC 3164?	ITMS 7.0 will be enhanced to add this capability		NIST SP 800-53 Audit and Accountability Elected Control
P.37	Does the product support filtering capabilities for all specified log types that are captured by the asset (e.g., application, database, network or system operating systems)?	ITMS 7.0 will be enhanced to add this capability		NIST SP 800-53 Audit and Accountability Moderate Baseline Requirement
P.38	Does the product support time stamps of transactions and events for purposes of logging?	Yes		NIST SP 800-53 Audit and Accountability Moderate Baseline Requirement
P.39	Does the product support encryption for data at rest?	Oracle deploys a very sophisticated HIPPA compliant encryption of data at rest.		NIST SP 800-53 Audit and Accountability Moderate Baseline Requirement
P.40	Does the product support data storage using encryption algorithms that exceed the strength of 128-bit advanced encryption standard?	Yes, Oracle deploys a very strong encryption standard (see reference: Data security)		NIST SP 800-53 Audit and Accountability Elected Control
P.41	Does the product or its configuration support the encryption of data in transit on the network?	Oracle encrypts data during transit via it SQL Client network protocol implementation		

P.42	Does the product support utilization of hashing and/or generally accepted digital signature based technology to provide non-repudiation of logs stored or transmitted from the asset including applications, database, network or system operating systems?	Yes		NIST SP 800-53 Audit and Accountability Elected Control
P.43	Does the product support the retention of log data for a preset period of time (in storage) as defined by Transit Authority?	Yes		NIST SP 800-53 Audit and Accountability Moderate Baseline Requirement
P.44	Does the product require unique user identification before access is granted to an asset including applications, databases, network or system operating platforms?	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement
P.45	Does the product require unique system identification before system-to-system access is allowed?	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement
P.46	Is the product capable of establishing user accounts based on unique attributes such as last names, initials, etc. at the discretion of Transit Authority?	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement
P.47	Is the product capable of restricting the permanent use of a unique user identifier that has already been used?	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement

P.48	Does the product require the authentication of a unique user identifier prior to permitting access to the requested resource?	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement
P.49	Is the product capable of supporting password strings of at least 15 characters during password authentication?	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement
P.50	Is the product capable of enforcing password complexity which requires the use of at least 1 uppercase, 1 lowercase, 1 special character, and 1 number?	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement

P.51	Is the product capable of enforcing that new passwords for unique user identifiers cannot use previous passwords?	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement
P.52	Does the product support password storage using at least 128-bit advanced encryption standard? If not, are the passwords saved in another secure method?	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement
P.53	Is the product capable of expiring passwords and requiring unique user identifiers to change their password after a preset period of time at the discretion of Transit Authority?	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement
P.54	Is the product capable of masking passwords during system entry? (i.e., shows passwords as ******).	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement
P.55	Does the product support cryptographic authentication schemes which are at a minimum in compliance with FIPS 140-2 (i.e. 128-bit AES for example is acceptable)?	Yes		NIST SP 800-53 Identification and Authorization Moderate Baseline Requirement
P.56	Is the product capable of separating the administration of the asset from the use of the asset (i.e., Application Partitioning) including applications, databases, network or system operating platforms?	Yes		NIST SP 800-53 System and Communications Protection Moderate Baseline Requirement
P.57	Is the product capable of restricting access from specific sources using specific protocols?	Yes all communication between applications and databases use industry standard and secure communication protocols such as Secure TCP/IP and		NIST SP 800-53 System and Communications Protection Moderate Baseline Requirement

		Oracle SQL*Net		
P.58	Does this product support checksums and hash values to	Oracle uses very stringent security protocol including supporting checksums and hash values		NIST SP 800-53 System

	maintain the integrity of information?			and Communications Protection Moderate Baseline Requirement
P.59	Is this product capable of encrypting data in transit to protect it from unauthorized disclosure?	ITMS 7.0 uses industry standard communication protocol such as SSL and Oracle SQL*Net to protect the information in transit.		NIST SP 800-53 System and Communications Protection
P.60	Is this product capable of terminating communications when sessions are completed?	Yes?		NIST SP 800-53 System and Communications Protection Moderate Baseline Requirement
P.61	Can the product be configured to communicate only with specific assets?	Yes		NIST SP 800-53 System and Communications Protection Elected Control
P.62	Is the product capable of utilizing PKI infrastructures? If	Yes		NIST SP 800-53 System and Communications Protection Elected Control
P.63	Is the product capable of utilizing only FIPS 140-2 compliant encryption algorithms (e.g., 128-bit AES)?	Yes		NIST SP 800-53 System and Communications Protection Elected Control

P.64	Does the product support protecting the data while being transmitted across the network? If so, what protection does it support	ITMS 7.0 uses industry standard communication protocol such as SSL and Oracle SQL*Net to protect the information in transit.		NIST SP 800-53 System and Communications Protection Elected Control
P.65	Does the product support the ability to use acceptable mobile code such as Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript?	Yes		NIST SP 800-53 System and Communications Protection Moderate Baseline Requirement
P.66	Does the product support session authenticity during initialization of sessions (e.g., SSL)?	ITMS 7.0 uses industry standard communication protocol such as SSL and Oracle SQL*Net to protect the information in transit.		NIST SP 800-53 System and Communications Protection Moderate Baseline Requirement
P.67	Does the system protect the confidentiality and integrity of the information at rest?	Oracle uses very stringent security protocol including supporting confidentiality and integrity of data at rest.		NIST SP 800-53 System and Communications Protection Moderate Baseline Requirement
P.68	Does the product support the ability to have vendor's correct flaws (e.g., security vulnerabilities) including applications, databases, network and system operating platforms?	Yes		NIST SP 800-53 System and Information Integrity Moderate Baseline Requirement
P.69	Is the product capable of being scanned using well-	Yes		NIST SP 800-53 System
	known antivirus systems for malicious code?	Yes		and Information Integrity Moderate Baseline Requirement

P.70	Is the product capable of restricting personnel from entering data in the asset based on access control (e.g., role-based access)?	Yes, ITMS 7.0 User Role Module restricts that access.		NIST SP 800-53 System and Information Integrity Moderate Baseline Requirement
P.71	Does the product have the ability to determine whether or not inputs are valid?	Input validation is built into the software fields.		NIST SP 800-53 System and Information Integrity Moderate Baseline Requirement
P.72	Does the product have the ability to identify potentially security-relevant error conditions and provide the information necessary for corrective actions?	ITMS 7.0 will produce error logs to indicate error conditons, but cannot discern by itself if the errors are security related. That will be done by HBSS staff.		NIST SP 800-53 System and Information Integrity Moderate Baseline Requirement