

CONTROL SURVEY						
Electronic Payments						
#	ASKD Domain	Security Control Requirement	Applicable Policy/Standard	Response	Comments	Short Name
						Applicable NIST 800-53 (Rev 4) Objective
1.1	Authentication & Identification (AN)	Does the application leverage a company's standard authentication control for providing single-sign-on capability?	Best Practice	No		User Authentication
1.2		Is multi-factor authentication as defined by the Information Security Standard leveraged for all users this application?	GISS Information Systems: 8.1.5	Yes		Multi-Factor Auth
1.3		Is multi-factor authentication as defined by the Information Security Standard leveraged for administrative users this application?	GISS Information Systems: 8.1.4	TBD		Multi-Factor Admin Auth
1.4		Are minimum password requirements for user accounts established in compliance with Information Security Standards?	GISS Information Systems: 7.2	No		Password Strength
1.5		Are service account credentials stored and managed using a Privileged Account Management solution?	GISS Information Systems: 6.6.3	Yes		Credential Management
1.6		Are passwords secured using hash + salt functions using strong cryptographic algorithms?	GISS Information Systems: 7.1.13 & 13.x	TBD		Secured Passwords
1.7		Are user accounts in the application locked out after a defined number of failed login attempts?	Best Practice	No		Account Lockout
2.1	Authorization / Access Control (AZ)	Is the process for provisioning and deprovisioning users within the application documented?	GISS Information Systems: 6.4	Yes		User Provisioning
2.2		Are users authorizations managed within a centralized tool?	Best Practice	TBD		User Authorization
2.3		Is a centralized list of all personnel with access to "SECRET" data established and maintained?	GISS Information Classification: Exhibit 1: Applicability	No		Secret Data Access
2.4	Configuration Security (CS)	Does the application use role-based access controls and principles of least privilege to assign user authorization?	GISS Information Systems: 6.2	Yes		RBAC
2.5		Are periodic reviews of user access rights conducted, at minimum, every six months?	GISS Information Systems: 6.7	TBD		Access Audits
3.1		Has the application been deployed on approved images or configurations and kept up to date using a patch management lifecycle?	GISS Information Systems: 4 & 5	No		Patch Management
3.2		Has a web application firewall been deployed and configured specifically for this application?	Best Practice	Yes		WAF Implementation
3.3		Does the application employ a multi-tiered design in which the presentation layer is isolated from other network segments?	Best Practice	TBD		Multi-tier Application Design
3.4		Is the application hosted on servers that are installed in a company owned data center or authorized secure facility?	0	No		Authorized Hosting
3.5		Is the application hosted on cloud service providers such as AWS, Azure, Google Cloud, etc.?	0	Yes		Cloud Hosted
3.6	Logging & Audit (LG)	Is the application protected by standard Anti-DDOS solution?	Best Practice	TBD		DDOS
4.1		Does the application log sufficient information regarding user successes and failures to reconstruct user activity?	GISS Information Systems: 10.2 & GISS Monitoring: 3.1	No		Logging
4.2		Are application logs written to a location that is protected from unauthorized access by systems personnel or other external parties?	GISS Monitoring: 3.5	Yes		Log Management
4.3		Is an automated log retention mechanism established to ensure the availability of log files?	GISS Information Systems: 10.3	TBD		Log Retention
4.4		Are application events forwarded to centralized and monitored SIEM with event notifications defined?	GISS Information Systems: 10.4	No		Log Events
4.5		Is user activity routinely reviewed to identify potential anomolous user activity or fraudulent use?	Best Practice	Yes		Log Activity Audits
5.1		Does the application make use of standard components for implementing anti-request forgery tokens?	Best Practice	TBD		Request Forgery
5.2	Request Forgery / Non-Repudiation (RF)	Do critical user actions (changing password, initiating a financial transaction, etc.) require re-authentication of the user?	Best Practice	No		ReAuthentication
6.1		Does the application leverage encryption on all communications channels that transmit Secret, Confidential or Personal data?	GISS Information Systems: 13.1.2	Yes		Encryption in Transit
6.2		Does the application leverage encryption to protect all Secret, Confidential or Personal data that is written to files?	GISS Information Systems: 13.1.3	TBD		File Encryption at Rest
6.3	Sensitive Data Protection (SD)	Does the application leverage encryption to protect all Secret, Confidential or Personal data that is written to databases?	GISS Information Systems: 13.1.3	No		DB Encryption at Rest
7.1		Are users sessions automatically terminated after a defined period of inactivity?	Best Practice	Yes		Session Inactivity
7.2		When user sessions are terminated, does the application remove all sensitive data from the screen/page or redirect the user to a new screen/page?	Best Practice	TBD		Session Termination
7.3	Session Management (SM)	Does the application make use of common libraries or components for generating and managing session identifiers?	Best Practice	No		SM Libraries
8.1		Does the application make use of any Anti-Cross Site Scripting or other common input validation libraries/components?	Best Practice	Yes		Anti XSS
8.2		Are acceptable/expected input characteristics defined for all data elements received from the user or other external systems?	Best Practice	TBD		Input Validation
8.3	Validation & Encoding (VE)	Is standard output encoding used on all user entered data returned to the user interface?	Best Practice	No		Output Encoding
9.1		Are reusable common libraries used for any typical application functionality (Authentication, Authorization, Logging, etc.)?	Best Practice	Yes		Common Libraries
9.2		Is the creation of design specifications, requirements definitions and other project artifacts enforced?	Best Practice	TBD		Sec Requirements
9.3	Extensible Design (XD)	Have common application functions been designed according to common design guidance or reference architectures?	Best Practice	No		Secure Design
10.1		Does the application undergo penetration testing on a monthly basis?	GISS Vulnerability Management: 8	Yes		Penetration Testing
10.2		Do application development teams submit application source code for a security review during the development lifecycle?	Best Practice	TBD		Code Review
10.3	Security Verification (SV)	Are Design Reviews/Threat Modeling conducted as part of the early concept phases of application development?	Best Practice	No		Threat Modeling
10.4		Are infrastructure level vulnerability scans performed against the application's servers consistent with the Information Security Standard on Vulnerability Management?	GISS Vulnerability Management: 8	Yes		Infrastructure Scans
10.5		Are infrastructure level vulnerability scans performed against the application's servers consistent with the Information Security Standard on Vulnerability Management?	GISS Vulnerability Management: 8	TBD		Infrastructure Scans
11.1	Third-Party Management (TM)	Has a vendor security assessment been performed against the vendor of this application?	GISS Third-Party Management: 4.1b	No		Vendor Assessment
11.2		Does the application's vendor provide regular security vulnerability updates to the organization?	Best Practice	Yes		Vendor Security Updates
11.3		Have vendor contracts been structured to include performance objectives and penalties for resolution of security vulnerabilities?	Best Practice	TBD		Vendor Contracts
11.4		Has the application vendor provided attestation of security assurance activities (vulnerability scans, penetration tests) conducted?	Best Practice	No		Vendor Attestation
11.5		Has the vendor signed a confidentiality agreement with Company?	GISS Third-Party Management: 3.1	Yes		Vendor NDA