A 23-062 - DISA Agreement
(DMV ISA)

Information security controls from NIST Special Publication 800-53; tailored to protect the confidentiality, integrity, and availability of DMV information and the information systems authorized to process, store, and transmit DMV information.

Legistar
DMV Version 2.0

INTRODUCTION

This document, the *Department of Motor Vehicles* (DMV) *Information Security Agreement* (ISA), must be completed by the organization that is requesting a connection to DMV. Your organization should coordinate with your Information Technology (IT) department and Information Security Officer (ISO) for completion. The DMV ISA uses information security standards and guidelines derived from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, to reinforce the information security requirements of the DMV for electronic access or connection.

Together, the NIST and DMV security requirements provide a robust baseline of security controls. These controls are essential for protecting the confidentiality, integrity, and availability of DMV information and the information systems authorized to process, store, and transmit that information.

The source of each DMV ISA control refers to a NIST SP 800-53 security control. The original NIST control numbers have been retained with each DMV ISA requirement, for ease of reference.

Hyperlinks are provided throughout this document for cross reference and clarification of terms.

COMPENSATING SECURITY CONTROLS

Generally, meeting compliance with the ISA requirements is a straight forward process. However, organizations may find some requirements impractical or not cost effective to implement; particularly when an organization has other controls already in place. In such instances, DMV may accept compensating controls. Compensating controls are alternative security controls considered sufficient to mitigate the risks framed by the ISA requirements.

For approval of compensating controls, submit additional information in the "Compensating Security Controls Section" located at the end of this questionnaire to provide supporting rationale for key points describing:

- *How* the compensating control provides security capabilities that are equivalent to the ISA security control, and
- *Why* the ISA security control cannot be implemented.

When compensating security controls are used, organizations need to accept the residual risk.

REQUIRED APPLICATION DOCUMENTS

1. The following documents are required *with* your DMV ISA:
   a. A diagram (topology) of your organization's information system, and all internal/external connections leading to and away from your organization's information system. The diagram must reflect the specific physical and logical (virtual) arrangement of the elements *used to access, process, transport, or store DMV information*. (See page 5)
   b. A written narrative of how DMV information flows through your Network from entrance to exit. (See page 5)
2. The following documents are required to be made *available* to DMV, upon request:
   a. Written policy and procedures for the security controls listed on page 9.
   b. A fully documented incident response plan (See Requirement IR-8/question #59).
   c. Required for consideration to connect: Valid requester account agreement which is combined with this document to become one (1) application.

APPLICATION TYPE (CHECK ALL THAT APPLY)	
☐ New	☐ Renewal
☐ Change Of Network Hardware/Software	☐ Change Of Number Of LUs
☐ Change Of Network Connections	☐ Change Of Network Location
☐ Proof Of Concept	☐ Other:

NAME/PHYSICAL ADDRESS OF YOUR ORGANIZATION	
Organization Name:	
Physical Address:	
City, State, Zip:	

ORGANIZATION CATEGORY & TYPE (CHECK ALL THAT APPLY)				
☐ Federal	☐ State	☐ County	☐ City	☐ Data Center
☐ Special District	☐ Higher Education	☐ Commercial	☐ Auto Club	☐ Other:

NAME/PHYSICAL ADDRESS OF YOUR DATA CENTER (IF APPLICABLE)	
Company Name	
Physical Address	
Type of Service	
Description of Service	
Name, Title, and Phone Number	

TYPE OF DMV INFORMATION RECEIVED	
☐ (DL) Driver License	☐ (FR) Financial Responsibility
☐ (VR) Vehicle/Vessel Registration	☐ (SS) Social Security (Full)
☐ (OL) Occupational Licensing	☐ (SS) Social Security (Match Only)
☐ Other (Specify):	

TYPE OF CONNECTIVITY TO/FROM DMV			
Connectivity Method	**OTech/DMV Gold Camp**	**OTech/DMV Vacaville**	**Data Center / Service Provider**
☐ Enterprise Extender Network	☐	N/A	☐
☐ Internet VPN	☐	☐	☐
☐ Internet VPN Telnet 3270	☐	N/A	☐
☐ Telnet 3270	☐	☐	☐
☐ T1/T2	☐	☐	☐
☐ Other:	☐	☐	☐

REQUIRED: Provide a detailed description of the type of connection/or change that is being requested (including, if applicable, number of LUs requested):

PURPOSE OF DMV INFORMATION
☐ Sell the information to the End-Users that originally requested the information.
☐ Use the information for your organization's own pre-approved business purposes.
☐ Pass the information to government entities that requested the information.
☐ Pass the information to commercial entities that requested the information.
☐ Other:

ACCESS TO REQUESTED DMV INFORMATION					
Does your organization have more than one (1) office or location? ☐ Yes ☐ No If so, how many other locations?					
Provide the address of all locations that access DMV information. (See page 4 for add'l locations)					
Main Location					
Name:					
Requester Code:					
Physical Address:					
City, State, Zip:					
# of Workstations:		Existing # of LUs:		Additional # of LUs requested:	
Workstation Type: ☐ PC ☐ Thin Client ☐ MAC ☐ Laptop ☐ 3270 Emulation ☐ Other (Specify):					
Operating System: ☐ Windows ☐ Apple ☐ Linux ☐ z/OS ☐ Unix ☐ SQL ☐ Oracle ☐ Other (Specify):					
Access Days/Hours/Holidays:					
Are any users able to access DMV information remotely (e.g., via mobile phones, home offices, laptops, Wi-Fi, VPN, Citrix, or Remote Desktop)? ☐ Yes ☐ No					
Is DMV information ***on your network*** sent to or accessed by any of the following? (Check all that apply) ☐ Vendors/contractors ☐ Individuals with business or legal authority (attorneys) ☐ Business Partners ☐ Other agencies – specify: ☐ Your organization's authorized staff					
Does your organization send DMV information to, store DMV information in, or administer systems containing DMV information from another country? ☐ Yes ☐ No					
Multi-Layer Authentication					
Does your organization use multi-layer or multi factor authentication when accessing DMV data? The following examples are acceptable: login ID with passwords to local network, login ID with passwords to DMV system, ID Tokens, Biometrics, or Magnetic Strip Cards, etc. ☐ Yes ☐ No					
Describe the first layer of user authentication:					
Describe the second layer of user authentication:					
Does your organization use password manager appliances? If so please describe the appliance:					

ADDITIONAL LOCATIONS					
Location #2					
Name:				Requester Code:	
Physical Address:					
City, State, Zip:					
# of Workstations:		Existing # of LUs:		Additional # of LUs requested:	
Workstation Type: ☐ PC ☐ Thin Client ☐ MAC ☐ Laptop ☐ 3270 Emulation ☐ Other (Specify):					
Operating System: ☐ Windows ☐ Apple ☐ Linux ☐ z/OS ☐ Unix ☐ SQL ☐ Oracle ☐ Other (Specify):					
Access Days/Hours/Holidays:					
Location #3					
Name:				Requester Code:	
Physical Address:					
City, State, Zip:					
# of Workstations:		Existing # of LUs:		Additional # of LUs requested:	
Workstation Type: ☐ PC ☐ Thin Client ☐ MAC ☐ Laptop ☐ 3270 Emulation ☐ Other (Specify):					
Operating System: ☐ Windows ☐ Apple ☐ Linux ☐ z/OS ☐ Unix ☐ SQL ☐ Oracle ☐ Other (Specify):					
Access Days/Hours/Holidays:					
Location #4					
Name:				Requester Code:	
Physical Address:					
City, State, Zip:					
# of Workstations:		Existing # of LUs:		Additional # of LUs requested:	
Workstation Type: ☐ PC ☐ Thin Client ☐ MAC ☐ Laptop ☐ 3270 Emulation ☐ Other (Specify):					
Operating System: ☐ Windows ☐ Apple ☐ Linux ☐ z/OS ☐ Unix ☐ SQL ☐ Oracle ☐ Other (Specify):					
Access Days/Hours/Holidays:					
Location #5					
Name:				Requester Code:	
Physical Address:					
City, State, Zip:					
# of Workstations:		Existing # of LUs:		Additional # of LUs requested:	
Workstation Type: ☐ PC ☐ Thin Client ☐ MAC ☐ Laptop ☐ 3270 Emulation ☐ Other (Specify):					
Operating System: ☐ Windows ☐ Apple ☐ Linux ☐ z/OS ☐ Unix ☐ SQL ☐ Oracle ☐ Other (Specify):					
Access Days/Hours/Holidays:					

If your organization has additional locations or branch offices that are included in your network and have access to DMV information, please identify below. Attach additional sheets if necessary.

If your organization utilizes third party contract services that store, process, or transmit CA DMV Data, please identify them below and describe the service provided to your organization. Services may include the following: Data Centers, Network Providers, Application Hosting, Cloud Computing, Application Development, Administration Support, etc… Attach additional sheets if necessary.

CONTRACTED SERVICES(S)	
CONTRACTED SERVICE #1	
Company Name	
Physical Address	
Type of Service	
Description of Service	
Contact Name, Title, and Phone Number	
CONTRACTED SERVICE #2	
Company Name	
Physical Address	
Type of Service	
Description of Service	
Contact Name, Title, and Phone Number	
CONTRACTED SERVICE #3	
Company Name	
Physical Address	
Type of Service	
Description of Service	
Contact Name, Title, and Phone Number	
CLOUD COMPUTING SERVICE	
Does your organization utilize Cloud Computing Services to store, process, or transmit CA DMV Data? ☐ Yes ☐ No	
If yes, is the cloud provider FedRAMP certified (Please visit **www.fedramp.gov** for additional reference and list of authorized/certified products or cloud services)? ☐ Yes ☐ No	
Company Name	
Physical Address	
Type of Service	
Description of Service	
Contact Name, Title, and Phone Number	

NETWORK TOPOLOGY SECTION

Every organization requesting access to DMV information is **required to provide a detailed Network Topology Diagram** and **Network Narrative** with their application of the logical and virtual information resources that are organized for processing, storing, and transmitting DMV information.

Network Topology Diagram: All network topologies are **required** to have firewalls, a Demilitarized Zone (DMZ), and Intrusion Detection Systems (IDS)/Intrusion Prevention System (IPS) identified on their diagram. **Each topology diagram must be dated and include the contact information of who prepared it**. **Attach a copy of your Network Topology Diagram to this application**.

Network Narrative: All network narratives are **required** to describe the route the DMV request follows from the time the end user initiates the request until the request is fulfilled and returned to the user. Narratives must describe in detail of the type of connection being used, and identify the flow of data through routers, switches, and firewalls. Narratives must also describe all pass through locations such as data centers, disaster recover/storage centers, third party vendors, and/or branch offices. **Attach a copy of your Network Narrative to this application**

Person Who Produced This Network Topology And Narrative				
Name	Position/Title	Email	Phone	Date

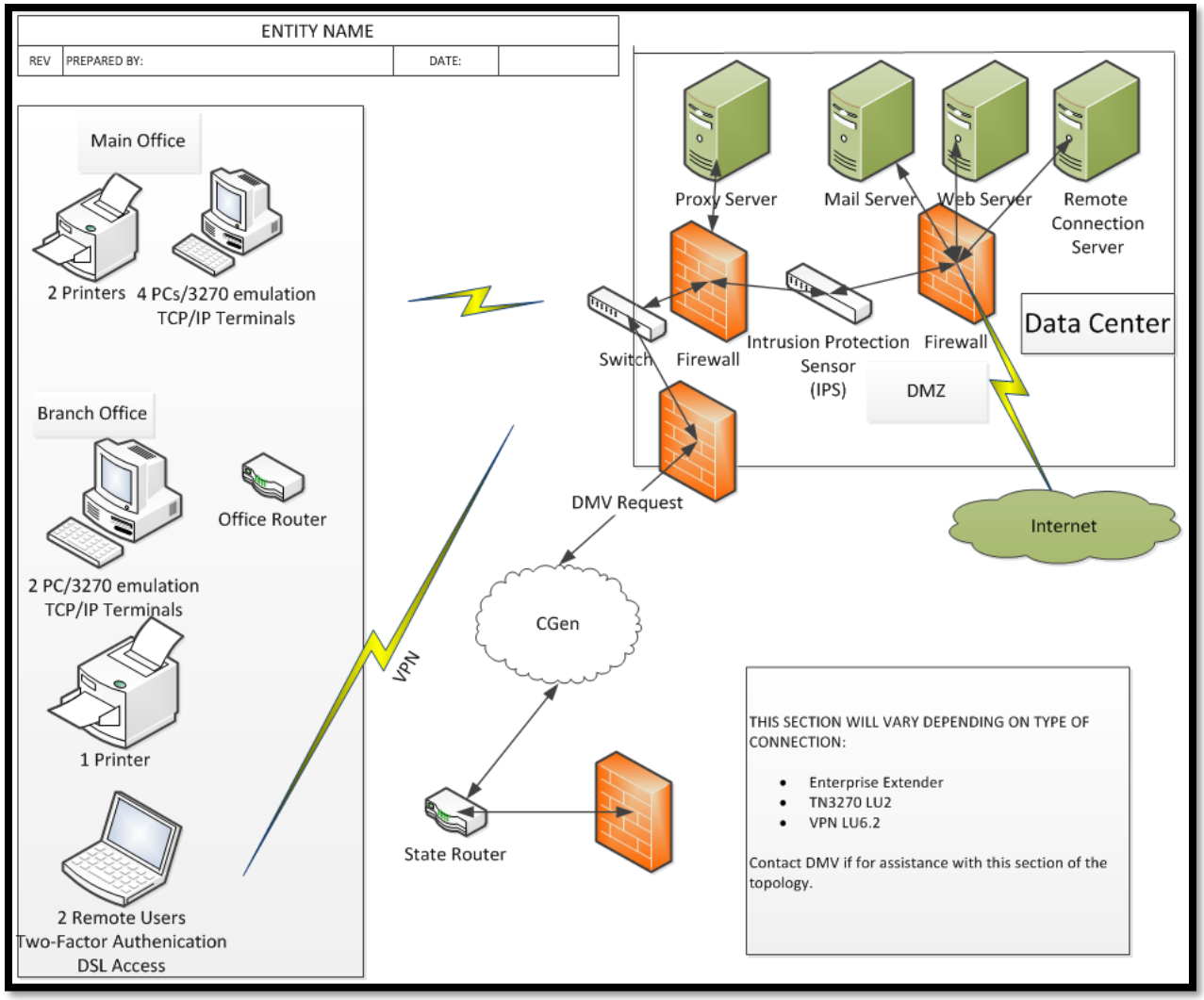
**Sample information resources and topology examples are provided below and on page 7 and 8 for reference:

INFORMATION RESOURCES

- Workstations (local and remote)
- Mainframes, Servers
- Front-End Processors
- Switches, Bridges, Router, Hubs
- Gateway Devices
- Storage Devices of DMV Data (If Applicable)
- Telecommuting Technology:
  - Dedicated Lines
  - Frame Relay
  - Data Link Control
  - Digital Subscriber Line (DSL)
  - Cable Modems
- Online Connections
- Database Locations
- Transport & Network Protocols
- Internet Connections
- Firewalls, DMZ, IDS, IPS
- Access Points of Outside LAN Providing DMV services
- Connections Points of Entities Processing/Transmitting DMV Data:
  - Commercial Access Control Administrator
  - OTech
  - Data Centers
  - Branch Offices
  - Third Parties

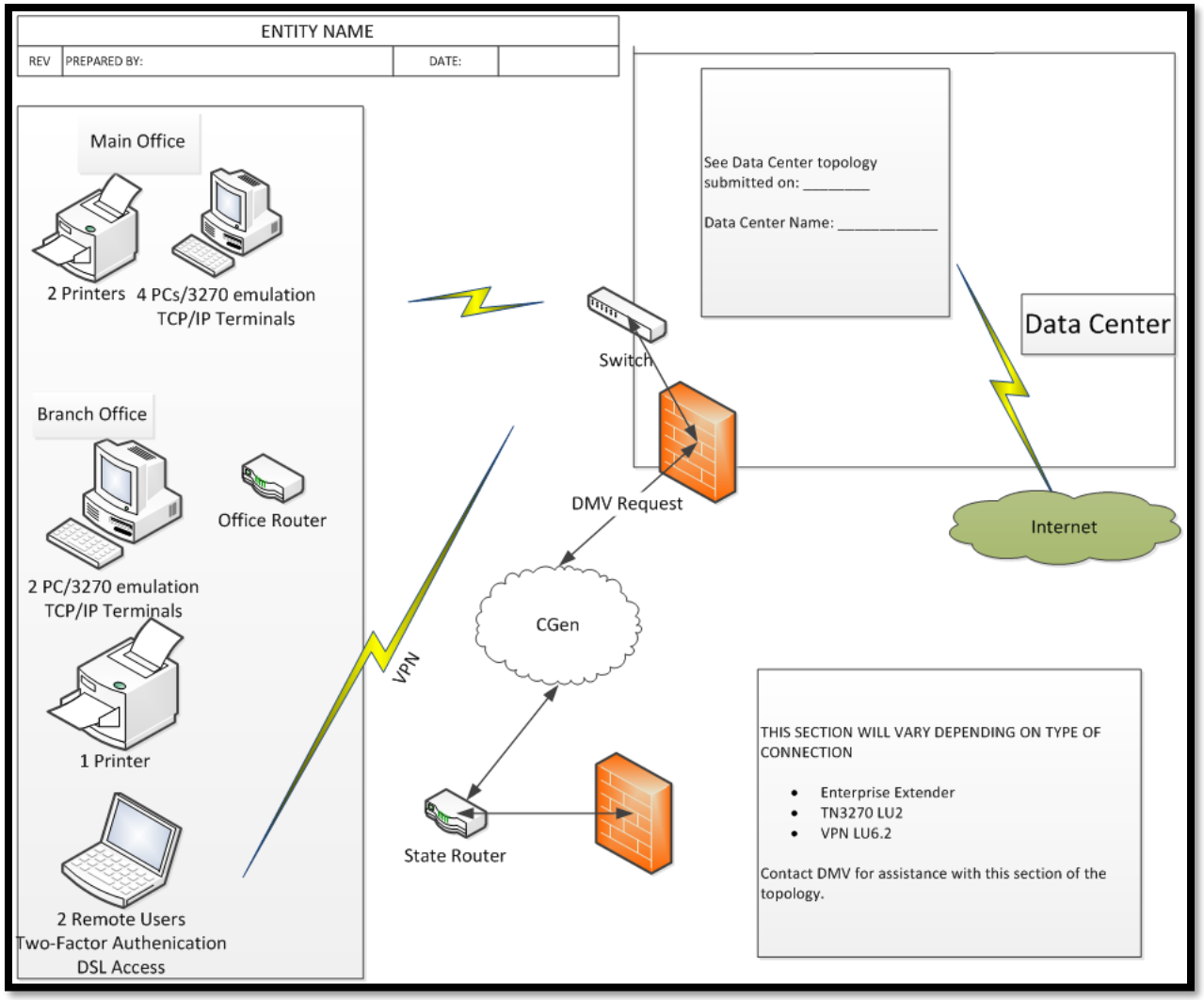
NETWORK TOPOLOGY SAMPLES

End User to DMV:



NETWORK TOPOLOGY SAMPLES (CONT.)

End User to Data Center:



REQUESTER CONTACT INFORMATION			
TECHNICAL			
Name	**Position/Title**	**Email**	**Phone**
BUSINESS			
Name	**Position/Title**	**Email**	**Phone**
SECURITY			
Name	**Position/Title**	**Email**	**Phone**

CERTIFICATION
The Requester certifies that the information contained in this DMV Information Security Agreement (DISA) and any supporting documentation is true and correct and accurately reflects the administration and security controls of the organization and the access to DMV Information and DMV Systems. The Requester also acknowledges that any contracted services that processes, stores, or transmits DMV information are fully compliant with the security controls identified in the DISA. Utilizing contracted services does not absolve the Requester of any responsibility for compliance with the DISA (must be signed by an authorized organization representative).
Signature: _____
Name:
Title:
Date:

FOR DMV USE ONLY			
DMV UNIT	**DMV ANALYST NAME**	**DATE APP RECEIVED**	**PHONE**
EAAU			
ISO			
ISD			
Comments:			

DMV ISA SECURITY POLICY AND PROCEDURES

The Department of Motor Vehicles requires every organization to have specified Security Policies and Procedures in place when accessing DMV information. Select the corresponding box if you have a policy or procedure for the specified security control. **If you do not have a policy or procedure, provide the date in the corresponding area as to when a policy or procedure will be in place for that specified security control.**

If your organization has compensating security policy/procedure, provide an explanation in the Compensating Security Controls Section located on the last page of this document.

POLICY AND PROCEDURES				
NIST #	**SECURITY CONTROL**	**Y**	**N**	**Will Be In Place By Date Below**
AC-#	Access Control	☐	☐	
AT-#	Awareness and Training	☐	☐	
AU-#	Audit and Accountability	☐	☐	
CA-#	Security Assessment and Authorization	☐	☐	
CM-#	Configuration Management	☐	☐	
IA-#	Identification and Authentication	☐	☐	
IR-#	Incident Response	☐	☐	
MA-#	Maintenance	☐	☐	
MP-#	Media Protection	☐	☐	
PE-#	Physical and Environmental Protection	☐	☐	
PS-#	Personnel Security	☐	☐	
RA-#	Risk Assessment	☐	☐	
SA-#	System and Services Acquisition	☐	☐	
SC-#	System and Communications Protection	☐	☐	
SI-#	System and Information Integrity	☐	☐	
	POLICY IMPLEMENTATION QUESTIONS	**Y**	**N**	
A	Are the policies distributed to all applicable staff?	☐	☐	
B	Are the policies reviewed and updated at least annually?	☐	☐	

DMV ISA SECURITY CONTROLS

All "**NO" responses require an implementation date** to indicate when full compliance is anticipated **along with a description of compensating security control** to supplement the NIST requirement. Descriptions of compensating security controls can be provided in the Compensating Security Controls Section located on the last page of this document. For additional information, clarification, or examples please refer to the associated NIST Control identified in the NIST Special Publication 800-53.

***Please Note:** The term, "Your Organization's Information System," is referenced throughout this document which describes all components (software/hardware) that are used to access DMV information from end point to end point (User to DMV data) as a whole.

	Access Control	Y	N	Will Be In Place By Date Below
Q. #	**Account Management – NIST AC-2**			
1	Does management of your organization's information system accounts, include the following? • Identifying account types (e.g., individual, group, system, application, guest/anonymous, and temporary). • Identifying authorized users of your information system and specifying access privileges. • Requiring appropriate approvals for requests to establish accounts. • Establishing, activating, modifying, disabling, and removing accounts. • Notifying account managers, when temporary accounts are no longer required and when users are terminated or transferred, or system usage changes are made. • Terminating or disabling on monthly basis: temporary, emergency, transferred/terminated users, and inactive accounts.	☐	☐	
2	Does your organization review user accounts at least annually?	☐	☐	
3	Does your organization's information system audit account creation, account modification, account disabling and termination actions, and notifies (as required) administrators and/or managers?	☐	☐	
	Access/Information Flow Enforcement – NIST AC-3/AC-4			
4	Does your organization's information system enforce permissions automatically between interconnected systems?	☐	☐	
	Separation of Duties – NIST AC-5			
5	Does your organization enforce separation of duties through assigned access authorizations?	☐	☐	
	Least Privilege – NIST AC-6			
6	Does your organization employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) necessary to accomplish authorized business functions?	☐	☐	

	Access Control (Continued)	Y	N	Will Be In Place By Date Below
	Unsuccessful Login Attempts - NIST AC-7			
7	Is the maximum number of consecutive invalid access attempts allowed by your organization's information system set between 3-5 attempts before locking out a user?	☐	☐	
8	Is the time period for lock-out mode or delay period set until user is authenticated and re-authorized by the system or system administrator?	☐	☐	
	System Use Notification – NIST AC-8			
9	Does your organization's information system display a system use notification message that displays the following? • System usage may be monitored, recorded, and subject to audit. • Unauthorized use of the system is prohibited and subject to administrative, criminal, and civil penalties.	☐	☐	
10	Does a notification banner remain on the screen until the user takes explicit actions to logon to the information system?	☐	☐	
	Session Lock - NIST AC-11			
11	Does your organization's information system initiate a session lock after 10-15 minutes of inactivity?	☐	☐	
12	Does your organization's information system allow a user to initiate a session lock that displays a screen saver or other display, hiding what was previously visible on the screen, when the session lock mechanism is activated?	☐	☐	
	Remote Access – NIST AC-17			
	Skip Questions 13-15 if you do not allow remote access to DMV information:			
13	Does your organization monitor for unauthorized remote access to your organization's information system?	☐	☐	
14	Does your organization enforce restrictions of remote connections to your organization's information system?	☐	☐	
15	Does your organization employ automated mechanisms (e.g., Intrusion Prevention System, Intrusion Detection System, Security Information Event Management System) to facilitate the monitoring and restriction of remote access methods?	☐	☐	
	Wireless Access Restrictions – NIST AC-18			
	Skip Questions 16-18 if you do not allow wireless access to DMV information:			
16	Does your organization enforce requirements for wireless access to your organization's information system?	☐	☐	
17	Does your organization monitor for unauthorized wireless connections and scans at least every three (3) months for unauthorized access points to the information system?	☐	☐	
18	Does your information system protect wireless access using authentication and encryption? (See IA-2 and SC-13).	☐	☐	

	Access Control (Continued)	Y	N	Will Be In Place By Date Below
	Mobile Devices – NIST AC-19			
	Skip Questions 19-21 if you do not allow mobile device access to DMV information:			
19	Does your organization monitor for unauthorized connections of mobile devices to your organization's information system?	☐	☐	
20	Does your organization enforce restriction of mobile device connectivity to your organization's information system?	☐	☐	
21	Does your organization prohibit the use of writable, removable media (DVDs, CDs, memory cards, USB devices, and external hard disk drives, etc.) to process, store or transmit DMV data?	☐	☐	
	AWARENESS AND TRAINING	Y	N	Will Be In Place By Date Below
	Security Awareness (Basic Information) – NIST AT-2			
22	Does your organization provide annual information security awareness training to all new and current authorized users (including managers, senior executives, and contractors) or when required by system changes?	☐	☐	
	Security Training Records – NIST AT-4			
23	Does your organization document information security training activities for each employee?	☐	☐	
	AUDIT AND ACCOUNTABILITY	Y	N	Will Be In Place By Date Below
	Content of Audit Records (Logs) – NIST AU-3			
24	Does your organization produce monthly audit records that contain sufficient information to establish the following? • The date and time of the DMV information request. • The end user identity making the request to DMV. • The type of information requested (e.g. VR, DL, FR, OL). • The points of identification used for the request (e.g., name, license number, date of birth). • The purpose of the request. • The transaction and information code.	☐	☐	
	Audit Monitoring, Analysis and Reporting – NIST AU-6			
25	Does your organization review and analyze your organization's information system audit records for indications of inappropriate or unusual activity, at least monthly?	☐	☐	
26	Does your organization promptly report findings of inappropriate or unusual activities to designated organizational officials and take necessary actions in response to the review/analyses of audit records?	☐	☐	
	Protection of DMV Audit Information NIST AU-9			
27	Does your organization protect DMV audit information and audit tools from unauthorized access, modification, and deletion?	☐	☐	

	AUDIT AND ACCOUNTABILITY (Continued)	Y	N	Will Be In Place By Date Below
28	Does your organization back up DMV audit records onto a system or media that is separate from your organization's information system?	☐	☐	
29	Does your organization use encryption to protect the integrity of audit records and audit tools?	☐	☐	
	Audit Record Retention- NIST AU-11			
30	Are monthly records of each request for information maintained for a period of two (2) years from the date of the request?	☐	☐	
	Skip Question 31 if you are not authorized to resell DMV information:			
31	Are monthly records of each request for information that is resold maintained for a period of five (5) years from the date of the request?	☐	☐	
	SECURITY ASSESSMENT AND AUTHORIZATION	Y	N	Will Be In Place By Date Below
	DMV Information Connections – NIST CA-3			
32	Does your organization document all DMV information system connections to external information systems (i.e., information systems such as branch/field offices or third-party business entities)?	☐	☐	
33	Does your organization authorize connections from your organization's information system to external information systems through the use of Interconnectivity Security Agreements?	☐	☐	
34	Does your organization monitor your organization's information system connections on an ongoing basis to verify enforcement of security requirements?	☐	☐	
	CONFIGURATION MANAGEMENT	Y	N	Will Be In Place By Date Below
	Configuration Change Control – NIST CM-3			
35	Are configuration-controlled changes to your organization's information system approved with explicit consideration for security impact analyses?	☐	☐	
36	Are configuration-controlled changes retained, documented, and reviewed?	☐	☐	
37	Are configuration-controlled changes tested and validated in a test environment before implementing the changes to your organization's production information system? **NOTE: Testing in the DMV production environment is prohibited.**	☐	☐	

	CONFIGURATION MANAGEMENT (Continued)	Y	N	Will Be In Place By Date Below
	Configuration Settings – NIST CM-6			
38	Does your organization define security configuration checklists, to be used for establishing and documenting mandatory configuration settings for technology products employed within your organization's information system?	☐	☐	
39	Does your organization monitor and control changes to the configuration settings in accordance with organization policies and procedures?	☐	☐	
	Least Functionality – NIST CM-7			
40	Is your organization's information system configured to: • Provide only essential capabilities? • Specifically prohibit and/or restrict the use of functions, ports, protocols, and/or services that are organization-defined as prohibited and/or restricted?	☐	☐	
41	Does your organization review your organization's information system firewall(s) and router configurations to identify and eliminate unnecessary functions, ports, protocols, and/or services at least every six (6) months?	☐	☐	
	DMV Information System Component Inventory – NIST CM-8			
42	Does your organization maintain and document the inventory of the components of your organization's information system to reflect the current state of the system?	☐	☐	
	IDENTIFICATION AND AUTHENTICATION	Y	N	Will Be In Place By Date Below
	Identification and Authentication (Organizational Users) – NIST IA-2			
43	Does each user, service account, and device have its own user ID? (no shared user IDs)	☐	☐	
44	Does your organization's information system use multi-layer or multi-factor authentication when accessing DMV data?	☐	☐	
	Identifier Management (User IDs) – NIST IA-4			
45	Does your organization: • Require authorization before issuing User IDs? • Prevent reuse of the User ID for 12 months? • Disable User ID after 60 days of inactivity? • Archive User ID?	☐	☐	

	IDENTIFICATION AND AUTHENTICATION (Continued)	Y	N	Will Be In Place By Date Below
	Authenticator Management (Token, PKI certificates, biometrics, passwords, key cards) – NIST IA-5			
46	Does your organization: • Verify the identity of the individual and/or device receiving the authenticator? • Require owners of user identifiers to choose their own passwords? • Require users to take specific measures to safeguard passwords, tokens and keycards? (i.e., if it is believed that a password has been disclosed, the user takes actions to change the password immediately.) • Establish administrative procedures for: a) Initial password, token, or keycard distribution? b) Lost/compromised or damaged passwords, tokens, or keycards? c) Revoking passwords, tokens, or keycards?	☐	☐	
47	Does your organization change default passwords upon your organization's information system installation?	☐	☐	
48	Does your organization encrypt stored passwords and/or biometric templates for user authentication with encryption strength equivalent to 256-bit or stronger?	☐	☐	
49	Does your organization's information system enforce the following password standards? • Passwords are automatically validated against user IDs, for DMV logon. • Passwords must consist of eight (8) or more characters. • Passwords consist of both alpha and numeric characters. • Passwords are not displayed in clear text. • Passwords contain special characters (e.g. @#$%^&*). • Passwords are changed at least every 45 to 90 days. • Users are required to obtain administrator authorization to change their password a second time. • Users are denied from re-using the same password within 12 password history iterations. • System-level passwords (e. g., root, enable, network, application, local, and enterprise-level administration) are required to be changed at least every three (3) months.	☐	☐	
	INCIDENT RESPONSE	Y	N	Will Be In Place By Date Below
	Incident Response Training – NIST IR-2			
50	Does your organization identify personnel with incident response roles and responsibilities?	☐	☐	
51	Does your organization provide incident response training to personnel?	☐	☐	

	INCIDENT RESPONSE (Continued)	Y	N	Will Be In Place By Date Below
52	Does your organization provide refresher incident response training at least annually?	☐	☐	
53	Does your Incident Response Training Material document defined tasks for each role?	☐	☐	
	Incident Monitoring – NIST IR-5			
54	Does your organization track and document security incidents?	☐	☐	
	Incident Reporting – NIST IR-6			
55	Does your organization meet requirements to instruct personnel to report, in one (1) business day, any suspected or actual DMV security incidents to DMV's Information Security Office at (916) 657-0201?	☐	☐	
56	Does your organization ensure reporting is consistent with the requirements of the California Information Practices Act of 1977 (California Civil Code§1798.29 and §1798.82a), listed below? • The types of incident information reported. • The content and timeliness of the reports. • The list of designated reporting authorities or organizations.	☐	☐	
	Incident Response Assistance – NIST IR-7			
57	Does your organization provide incident handling and reporting awareness to all users?	☐	☐	
	Incident Response Plan – NIST IR-8			
58	Does your organization have an incident response plan that defines reportable incidents, identifies classes of incidents (e.g., malware infestation, violation of security policy, acceptable user policy), defines response tasks, define responsible personnel for each class of incident, and is reviewed and approved by designated officials within the organization?	☐	☐	
59	Does your organization review, revise, and distribute copies of the incident response plan at least annually?	☐	☐	
	MAINTENANCE	Y	N	Will Be In Place By Date Below
	Controlled Maintenance– NIST MA-2			
60	Does your organization schedule, perform, document, and review maintenance and repair records on DMV information system components?	☐	☐	
61	Does your organization control all maintenance activities, whether performed on site, remotely, or removed to another location?	☐	☐	
62	Does your organization require a designated official to approve the removal of you organization's information system components from your facilities for off-site maintenance or repairs?	☐	☐	
63	Does your organization sanitize equipment to remove all DMV and sensitive information prior to removal from your facilities for offsite maintenance or repair?	☐	☐	

	MAINTENANCE (Continued)	Y	N	Will Be In Place By Date Below
64	Following maintenance or repair actions, does your organization check all security controls to verify that the controls are still functioning properly?	☐	☐	
65	Do maintenance records for your organization's information system include the following? • The date and time of maintenance. • Name of the individual performing the maintenance. • Name of the employee escorting the vendor (if applicable). • Description of the maintenance performed. • List of equipment removed or replaced (including identification numbers, if applicable).	☐	☐	
	Maintenance Tools– NIST MA-3			
66	Does your organization check all media containing diagnostic test programs for malicious code before the media are used in your network (e.g., software or firmware used for maintenance or diagnostics)?	☐	☐	
	Remote (e.g. Off-site, Third Party) Maintenance – NIST MA-4			
	Skip Questions 67-69 if you do not allow remote access to DMV information:			
67	Does your organization maintain records for remote maintenance and diagnostic activities?	☐	☐	
68	Does your organization terminate all sessions and your organization's information system connections when remote maintenance or diagnostics is completed?	☐	☐	
69	Do designated personnel within your organization audit remote maintenance/diagnostic sessions and review maintenance records of remote sessions?	☐	☐	
	MEDIA PROTECTION	Y	N	Will Be In Place By Date Below
	Media Access – NIST MP-2			
70	Does your organization restrict access to your organization's information system media storage and storage areas to authorized individuals?	☐	☐	
71	Does your organization audit access attempts and access entries into media storage areas?	☐	☐	
72	Does your network use 256-bit strength cryptography mechanisms to protect access to DMV information on portable digital media (e.g., laptops, smart phones, USB drives, tablets, DVD, or CDs)?	☐	☐	
	Media Storage – NIST MP-4			
73	Does your organization prevent DMV information from being electronically stored, combined, or linked with another database's information for resale or for any purpose not previously approved by DMV?	☐	☐	

	MEDIA PROTECTION (Continued)	Y	N	Will Be In Place By Date Below
74	Is DMV information not stored beyond its intended business purpose, unless mandated by Federal or State record retention requirements?	☐	☐	
75	Is DMV information media protected until the media is destroyed or sanitized using NIST approved techniques and procedures? (See NIST SP 800-88)	☐	☐	
	Media Sanitization – NIST MP-6			
76	Does your organization sanitize digital media identified as containing DMV information prior to disposal, release out of organizational control, and release for reuse?	☐	☐	
77	Does your organization track, document, and verify sanitization and disposal actions?	☐	☐	
78	Do sanitization procedures meet NIST 800-88 requirements for Personally Identifiable Information?	☐	☐	
	PHYSICAL AND ENVIRONMENTAL PROTECTION	Y	N	Will Be In Place By Date Below
	Physical Access Authorizations – NIST PE-2			
79	Does your organization develop and keep current list of personnel with authorized access to the facility where your organization's information system resides?	☐	☐	
80	Does your organization review and approve the physical access list and authorization credentials for the facility at least annually?	☐	☐	
81	Does your organization issue authorization credentials (e.g., badges, identification cards, smart cards)?	☐	☐	
	Physical Access Control – NIST PE-2			
82	Does your organization verify employee identity and what areas they are authorized to access before granting access to the facility?	☐	☐	
83	Does your organization control entry to the facility containing your organization's information system using physical access devices (e.g., keys, locks, combinations, card readers)?	☐	☐	
84	Does your organization: • Secure and regularly inventory keys, combinations, and other access devices? • Change combinations and keys as needed? • Change keys when lost or combinations compromised? • Change keys and combinations when individuals are transferred or terminated?	☐	☐	
	Access Control for Transmission Medium – NIST PE-4			
85	Does your organization control physical access to network distribution and transmission lines within your facility?	☐	☐	

	PHYSICAL AND ENVIRONMENTAL PROTECTION (Continued)	Y	N	Will Be In Place By Date Below
	Access Control for Output Devices – NIST PE-5			
86	Does your organization control physical access to output devices (e.g., monitors, printers, copiers) to prevent unauthorized individuals from obtaining the output?	☐	☐	
	Monitoring Physical Access – NIST PE-6			
87	Does your organization review physical access logs for your organization's information system at least monthly?	☐	☐	
88	Does your organization monitor real-time intrusion alarms and surveillance equipment?	☐	☐	
	Visitor Access Records – NIST PE-8			
89	Does your organization maintain physical access records of visitors that include the information below? • Name and organization of the visitor. • Signature of the visitor. • Type of identification presented (e.g., DL, badge). • Date of access. • Time of entry and departure. • Purpose of visit. • Name and location of person visited.	☐	☐	
	Delivery and Removal – NIST PE-16			
90	Does your organization maintain records of DMV information asset components (e.g., hardware, firmware software) items entering and exiting the facility?	☐	☐	
	Location of DMV Information System Components – NIST PE-18			
91	Are your organization's information system components (e.g., monitors, servers) physically positioned within the facility so as to minimize the opportunity for unauthorized viewing and access?	☐	☐	
	PERSONNEL SECURITY	Y	N	Will Be In Place By Date Below
	Personnel Termination – NIST PS-4			
92	Does your organization terminate DMV access upon termination of an individual's employment?	☐	☐	
93	Does your organization conduct Exit Interviews and all DMV related property (e.g., key fobs, laptops) is retrieved from terminated personnel?	☐	☐	
	Personnel Transfer – NIST PS-5			
94	Does your organization review electronic and physical access authorizations to DMV information and terminate accesses when personnel are reassigned or transferred to other positions within the organization?	☐	☐	

	PERSONNEL SECURITY (Continued)	Y	N	Will Be In Place By Date Below
	Access Agreements – NIST PS-6			
95	Does your organization **require all individuals** (employees, contractors, or agents) having direct or incidental access to DMV information and /or to your organization's information system to sign the Information Security Statement (form INF1128) prior to authorizing access and annually thereafter (includes employees of county data centers and the Administrative Offices of the Courts)?	☐	☐	
96	Does your organization retain all INF 1128 forms at the worksite for audit purposes?	☐	☐	
97	Does your organization retain the INF 1128 forms for a period of two (2) years after an employee is terminated, leaves the organization or if the office closes?	☐	☐	
	Third Party Personnel Security – NIST PS-7			
98	Does your organization establish personnel security requirements, security roles and responsibilities for third-party providers (e.g., contractors, information technology services, outsourced applications, network security management)?	☐	☐	
	Personnel Sanctions – NIST PS-8			
99	Does your organization establish formal sanctions process for personnel failing to comply with established DMV information security policies and procedures?	☐	☐	
	RISK ASSESSMENT	Y	N	Will Be In Place By Date Below
	Risk Assessment– NIST RA-3			
100	Does your organization perform a risk assessment on the organization's information system and the information it process, stores, or transmits?	☐	☐	
101	Does your organization update the risk assessment whenever there are significant changes to the organization's information system or environment of operation, or other conditions that may impact the security state of the system?	☐	☐	
	Vulnerability Scanning – NIST RA-5			
102	Does your organization conduct vulnerability scanning within your organization's information system and hosted applications at least every three (3) months, and/or when significant new vulnerabilities potentially affecting the system are identified and reported?	☐	☐	
103	Does your organization compare the results of vulnerability scans over time, to determine trends in your organization's information system vulnerabilities?	☐	☐	
104	Does your organization remediate legitimate vulnerabilities in accordance with the organization's pre-defined response times and procedures?	☐	☐	

	SYSTEM AND SERVICES ACQUISITION	Y	N	Will Be In Place By Date Below
	DMV Information System Documentation (Topology & Narrative) – NIST SA-5			
105	Will your organization maintain, and upon request, provide DMV with a written descriptive account with sufficient detail to permit analysis of the following below? • The secure configuration, installation, and operation of your organization's information system. • The effective use and maintenance of security features/functions. • The flow of DMV information in your organization from entrance to exit.	☐	☐	
106	Will your organization meet the requirement to maintain and upon request, provide DMV with a network topology/diagram with sufficient detail to permit analysis of the following components? • security components • servers • switches • gateway devices • firewalls • routers • connection points • workstations • internet connections • transport and network protocols used • VPN connections • access points outside the organization providing DMV services	☐	☐	
	External Information System Services – NIST SA-9			
	Skip Questions 107-108 if you do not contract with third party services and/or vendor:			
107	Does your organization require providers of external information system services to comply with the DMV ISA information security requirements and employ organization-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance?	☐	☐	
108	Does your organization monitor security control compliance by external service providers?	☐	☐	
	Developer Configuration Management – NIST SA-10			
109	Are your organization's information system developers required to create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation?	☐	☐	

	SYSTEM AND SERVICES ACQUISITION (Continued)	Y	N	Will Be In Place By Date Below
	Developer Security Testing – NIST SA-11			
110	Does your organization require your organization's information system developers (and system integrators) to create and implement a security test and evaluation plan, implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process, and document the results of the security testing/evaluation and flaw remediation processes?	☐	☐	
	SYSTEM AND COMMUNICATIONS PROTECTION	Y	N	Will Be In Place By Date Below
	Application Partitioning – NIST SC-2			
111	Does your organization separate User functionality from your organization's information system management (System Administrator) functionality?	☐	☐	
	DMV Information in Shared Resources– NIST SC-4			
112	Does your organization prevent unauthorized and unintended DMV information transfers via shared system resources?	☐	☐	
	Boundary Protection – NIST SC-7			
113	Does your organization monitor and control communications at the access points of your organization's information system?	☐	☐	
	Transmission Integrity – NIST SC-8 and SC- 9			
114	Does your organization's DMV information system protect the integrity of DMV information during transmission, protect the confidentiality of DMV information during transmission, and employ cryptographic mechanisms to prevent unauthorized disclosure of DMV information during transmission?	☐	☐	
	Network Disconnect – NIST SC-10			
115	Does your organization's information system terminate a network connection after end of session and 10 minutes of inactivity?	☐	☐	
	SYSTEM AND COMMUNICATIONS PROTECTION (Continued)	Y	N	Will Be In Place By Date Below
	Use of Cryptography – NIST SC-13			
116	Does your organization's information system implement cryptographic protection in storage and during transmission that comply with applicable laws, directives, policies, regulations, standards, and guidance for DMV information that is classified as personally identifiable information (PII)?	☐	☐	
	Session Authenticity – NIST SC-23			
117	Does your organization's information system disable session identifiers (e.g., session token, cookies) upon user logout or other session termination?	☐	☐	

	SYSTEM AND INFORMATION INTEGRITY	Y	N	Will Be In Place By Date Below
	Malicious Code Protection – NIST SI-3			
118	Is your organization's information system implemented with malicious code protection?	☐	☐	
119	Does your organization employ malicious code protection mechanisms to detect and eradicate malicious code in critical entry and exit points, workstations, and servers of your organization's information system?	☐	☐	
120	Does your organization update malicious code protection mechanisms whenever new releases are available and include the latest malicious code definitions in accordance with organizational configuration management policy and procedures?	☐	☐	
121	Does your organization's malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Web access, removable media, or other common means; or when inserted through the exploiting of information system vulnerabilities?	☐	☐	
	DMV Information System Monitoring – NIST SI-4			
122	Does your organization employ tools and techniques to monitor events, detect attacks, and identify unauthorized use on your organization's information system?	☐	☐	
123	Does your organization deploy monitoring devices to strategically collect essential information, track specific types of transactions at ad hoc locations, and track impact of security changes made to your organization's information system?	☐	☐	
124	Does your organization identify incident response personnel by name and/or by role and are notified of suspicious events?	☐	☐	
	Skip Questions 125-126 if you do not allow wireless access to DMV information:			
125	Does your organization employ a wireless intrusion detection system to identify rogue wireless devices, detect attack attempts, and detect potential compromises/breaches?	☐	☐	
126	Does your organization's information system monitor for unusual or unauthorized activities or conditions of inbound and outbound communications?	☐	☐	
	DMV Information System Monitoring Security Alerts, Advisories, and Directives – NIST SI-5			
127	Does your organization receive security alerts/advisories on a regular basis, issue security alerts/advisories to appropriate personnel, and take appropriate actions in response to security alerts/advisories for your organization's information system?	☐	☐	

	SYSTEM AND INFORMATION INTEGRITY (Continued)	Y	N	Will Be In Place By Date Below
	Software and Information System Integrity – NIST SI-7			
128	Does your organization employ centrally managed integrity verification tools (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) to monitor the integrity of the organization's information system and the applications hosted?	☐	☐	
129	Does your organization employ automated/manual tools to provide notification to designated individuals upon discovering unauthorized changes to your organization's information system?	☐	☐	
	Spam Protection – NIST SI-8			
130	Does your organization employ spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by email, email attachments, Internet accesses, or other common means at the following locations? • At your organization's information system entry and exit points. • At workstations. • At servers. • At mobile computing devices on the network.	☐	☐	
131	Does your organization update spam protection mechanisms when new releases are available?	☐	☐	
	Error Handling – NIST SI-11			
132	Does your organization generate error messages that are revealed only to authorize individuals, without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries?	☐	☐	

COMPENSATING SECURITY CONTROL SECTION

For every "No" response, please provide detailed descriptions for any compensating security policies, procedures, or controls that your organization uses in place of the recommended requirements stated in this agreement.

COMPENSATING SECURITY POLICIES AND PROCEDURES	
NIST #	Description

COMPENSATING SECURITY CONTROLS	
Question #	Description