California Health Center Security Grant Program (CHCSGP)
Re-Appropriation

FY 2019 Vulnerability Assessment Worksheet

The FY 2019 CHCSGP Request for Proposal (RFP) requires the submission of a Vulnerability Assessment (VA) as part of the application package. Assessments should cover such general areas as threats, vulnerabilities and mitigation options, consequences, perimeter, lighting, and physical protection, etc., as contained in the VA Worksheet.

This VA Worksheet must be completed as a record of the vulnerability assessment, and returned with your grant application.

Section 1 - Name of each Assessor and any associated professional credentials (Such as CPP, PSP, TLO, military, other security, inspection or auditing credentials)	**Signature of the Assessor**	**Date of Assessment**

Section 2 - Applicant General Information	
Attach an aerial photo of the site that clearly shows the property line and all structures. *(Use an online mapping program to create an aerial photograph of the site.)*	
Dun and Bradstreet (DUNS) Number:	
GPS Latitude & Longitude: *(Use an online mapping program to create an aerial photograph of the site.)*	
Local Law Enforcement Agency: (Name & Address)	
Local Fire Department: (Name & Address)	

Threat Assessment:

When possible, the vulnerability assessor(s) for the grant should coordinate with local law enforcement, the regional fusion center, and/or Urban Area Security Initiative (UASI) representatives to get a clear picture of the current threats.

Overall Description of Threat(s):	
List any criminal acts against persons or property directed at the site initiated to achieve political or social objectives during the last 5 years. Attach any photos, news articles or police reports that validate the incidents.	
Incidents	**Describe the Impact to the site**
1.	
2.	
3.	
4.	
5.	
6.	

VA Template

This VA template is provided to assist assessors and Applicants in collecting security-related data on the organization and site. Please complete and return this Annex with your grant application. Submitted VAs should cover the same general areas such as threats, vulnerabilities and mitigation options, consequences, perimeter, lighting, and physical protection, etc.

Assessors and Applicants should collectively discuss these security-related questions during the assessment phase of the VA. This inclusive approach will help the Applicant complete the grant application and help the organization become more aware of the risks to the site.

Perimeter and Access Control Assessment	
Does the site, facility, or installations have a clearly defined perimeter? Is this perimeter boundary posted? **(Yes or No/Describe if appropriate.)**	
Does the site have perimeter fencing, and is this fencing maintained? Is the perimeter fence clear of vegetation and debris? Do	

Perimeter and Access Control Assessment	
you have a clear line of site through the perimeter fence? **(Yes or No/ Describe if appropriate or attach photos.)**	
Are there known deficiencies in the security perimeter? Are deficiencies being corrected? What is the status? **(Yes or No/ Describe if appropriate or attach photos.)**	
Are Intrusion Detection System (IDS) sensors integrated into perimeter property line protection? **(Yes or No/Describe if appropriate.)**	
Does the organization effectively address all vehicle and pedestrian entry and exit points? Does the site, facility, or installation have high-speed avenues of approach? **(Yes or No/Describe if appropriate.)**	
Does the site, facility, or installations have illumination at any or potential security checkpoints to examine credentials, personnel, and vehicle? **(Yes or No/Describe if appropriate.)**	
Is the perimeter checked routinely by staff, volunteers, members, or security? **(Yes or No/Describe if appropriate.)**	

Security Lighting	
Are doorways illuminated for security and safety? **(Yes or No/Describe if appropriate.)**	
Are pathways around the site illuminated to assist with movement and safety? **(Yes or No/Describe if appropriate.)**	
Is the lighting adequate to assist the security camera system to detect, identify activities around the site? **(Yes or No/Describe if appropriate.)**	
Are all identified critical areas covered by lights? Is the lighting adequate from a security perspective at roadway access and parking areas? **(Yes or No/Describe if appropriate.)**	
Does vegetation or debris obstruct illumination and or create dark shadows? **(Yes or No/Describe if appropriate.)**	

Security Intrusion Detection/Security Camera System/Fire System	
Does the site, facility, or installations have a security center? Does the security center have adequate access control and alarm procedures? Is the security control center highly visible and has a secondary center been identified if the first one is affected by an incident? **(Yes or No/Describe if appropriate.)**	
Does the site have an IDS installed on all windows, doors, skylights, crawl spaces, and roof hatches? **(Yes or No/Describe if appropriate.)**	
Does the IDS provide any specific or more focused coverage of identified critical assets? **(Yes or No/Describe if appropriate.)**	
Does the site have a security camera system in place? **(Yes or No/Describe if appropriate.)**	
Are all facility critical assets under security camera system coverage? **(Yes or No/Describe if appropriate.)**	
Are the security camera feeds and/or IDS systems monitored? (e.g. on-site, offsite, mobile) **(Yes or No/Describe if appropriate.)**	
Are the security cameras and IDS sensors integrated in order to detect, identify, and respond to alarm activations? **(Yes or No/Describe if appropriate.)**	
Does the physical security protection system integrate the lights, cameras, fire alarms, and other sensors into a manageable security system? **(Yes or No/Describe if appropriate.)**	
Do the facility's systems directly communicate with local law enforcement and fire? **(Yes or No/Describe if appropriate.)**	

Security Operations	
Does the facility use a security company, employees, volunteers, or members to perform security patrol operation? **(Yes or No/Describe if appropriate.)**	
Are entry control visual inspections evident at entry points? **(Yes or No/Describe if appropriate.)**	
Are after hours checks made of the facility by employees, volunteers, or members? **(Yes or No/Describe if appropriate.)**	
Are the observations of the patrol documented in a daily security log? **(Yes or No/Describe if appropriate.)**	
Are there procedures for reporting suspicious personnel or activities? **(Yes or No/Describe if appropriate.)**	
Is there an effective employee entry control badge system, visitor pass system, or visitor escort policy and procedure? **(Yes or No/Describe if appropriate.)**	
How does the organization communicate with employees, volunteers, and members during emergencies? **(Describe.)**	

Vulnerability Assessment Attachment List (e.g. photographs, maps, diagrams)

Mitigation Options:

This section is designed to help the Applicant identify vulnerabilities, consider potential consequences, and select target hardening (mitigation) options to complete the application. Not all vulnerabilities identified during the assessment are critical to the operation of the organization and may not be listed.

Mitigation options and consequences must be listed with the vulnerabilities. This section is used to validate requests for specific equipment in the current grant application.

List the vulnerabilities that could be exploited through threats directed at the organization. Also, provide a mitigation option for the vulnerabilities. This data will assist the grant Applicant in identifying the vulnerabilities and consider target hardening options to complete the application.
List the site's vulnerabilities, mitigation options, and potential consequences. Mitigation Options should describe and include equipment that will be requested for purchase as part of the grant application.
Vulnerability: Mitigation Options: (Target Hardening)
Vulnerability: Mitigation Options: (Target Hardening)
Vulnerability: Mitigation options: (Target Hardening)
Vulnerability: Mitigation options: (Target Hardening)
Vulnerability: Mitigation options: (Target Hardening)
Vulnerability: Mitigation options: (Target Hardening) Potential Consequences: (specific to the organization)
Vulnerability: Mitigation options: (Target Hardening)