

Appendix II.A for the United States

**Regional Procedures and Guidelines for State, Local, Tribal and Public
Security/Safety Organizations in the United States to access the Cross Border
Security Communications Network along the Common Border**

Regional Procedures and Guidelines for Requesting and Granting Access to the CBSCN finalized on the ____ day of ____ 2014.

SECTION I. PREFACE

This document establishes regional policies and procedures for granting access of State, Local, Tribal and Similar Public Security/ Safety Organizations along shared borders to the Cross Border Security Communications Network (CBSCN). As stated in the *Protocol Between the Department of State of the United States of America and the Secretariat of Communications and Transportation of the United Mexican States Concerning the Use of Radio Frequencies by Certain Fixed Terrestrial links Constituting a Cross Border Public Security Communications Network Along the Common Border* (2009 Protocol), the network is “established to enhance the interoperability of public security communications on each side of the common border for the purpose of improving border security and combating border violence.”

In coordination with the United States and Mexico leaders of the High Level Consultative Commission on Telecommunications (HLCC), the CBSCN was developed as a long-term international cross border communications solution. The United States and Mexico identified ten city-pair locations along the common international border for these cross border systems. These locations were chosen based on their proximity to each country’s available microwave sites, geographical diversity, and the ability of State, local and tribal law enforcement and public safety agencies to access the sites for future interconnection and cross border communications. The intent is for these network connections to initially be used to support communications between U.S. Federal agencies and like agencies in Mexico, and to also allow State, local, and tribal law enforcement and public safety agencies access to the network.

This document does not develop any international treaty or agreement reserved for Federal jurisdiction by either country. Rather, it establishes procedures and methods for State, Local, Tribal and Public Security/Safety Organizations to gain authorized access, and continued use of the CBSCN while building on the provisions established in the 2009 Protocol and Procedure and Guidelines signed July 23, 2013.

SECTION II. REQUESTS FOR NETWORK ACCESS AND USE BY U.S. STATE, LOCAL, TRIBAL AND PUBLIC SECURITY/SAFETY ORGANIZATIONS

Each State, Local, Tribal, and Public Security/Safety Organizations will submit an application (Attachment A) for network access to their designated Statewide Interoperability Coordinator (SWIC) or SWIC representative. The SWIC or SWIC representative will review and approve the request prior to submitting the application to the Office of Emergency Communications (OEC) Representative via the Southwest Border Communications Working Group (SWBCWG) Homeland Security Information Network (HSIN) site, with a notification email to oc@hq.dhs.gov. Agencies shall ensure the application includes the type of access being requested, a description of how the agency plans to connect to the CBSCN, and identify which agencies/organizations within Mexico they wish to connect to, as per Attachment A. Only fully documented applications will be accepted by the OEC Representative for processing. Emails containing the applications should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, the information may be transmitted over regular email channels. For added security, when transmitting the application over a regular email channel, the information can be included as a password protected attachment with the password provided under separate cover.

Once the application has been submitted via the SWBCWG HSIN site, the OEC representative will coordinate as necessary with the requesting agency and/or the SWIC or SWIC representative with any questions prior to submission of the application at the Bi-National Working Group (BWG). The BWG will make the final determination regarding access to the CBSCN and inform the OEC

headquarters representative of the decision. The OEC representative will notify the requesting agency, the SWIC or SWIC representative, and the respective OEC Coordinator of the final determination regarding CBSCN access and the follow on of expectations of the next phase. It is the responsibility of the requesting agency to then begin the acquisition and coordination with CBP during the implementation phase.

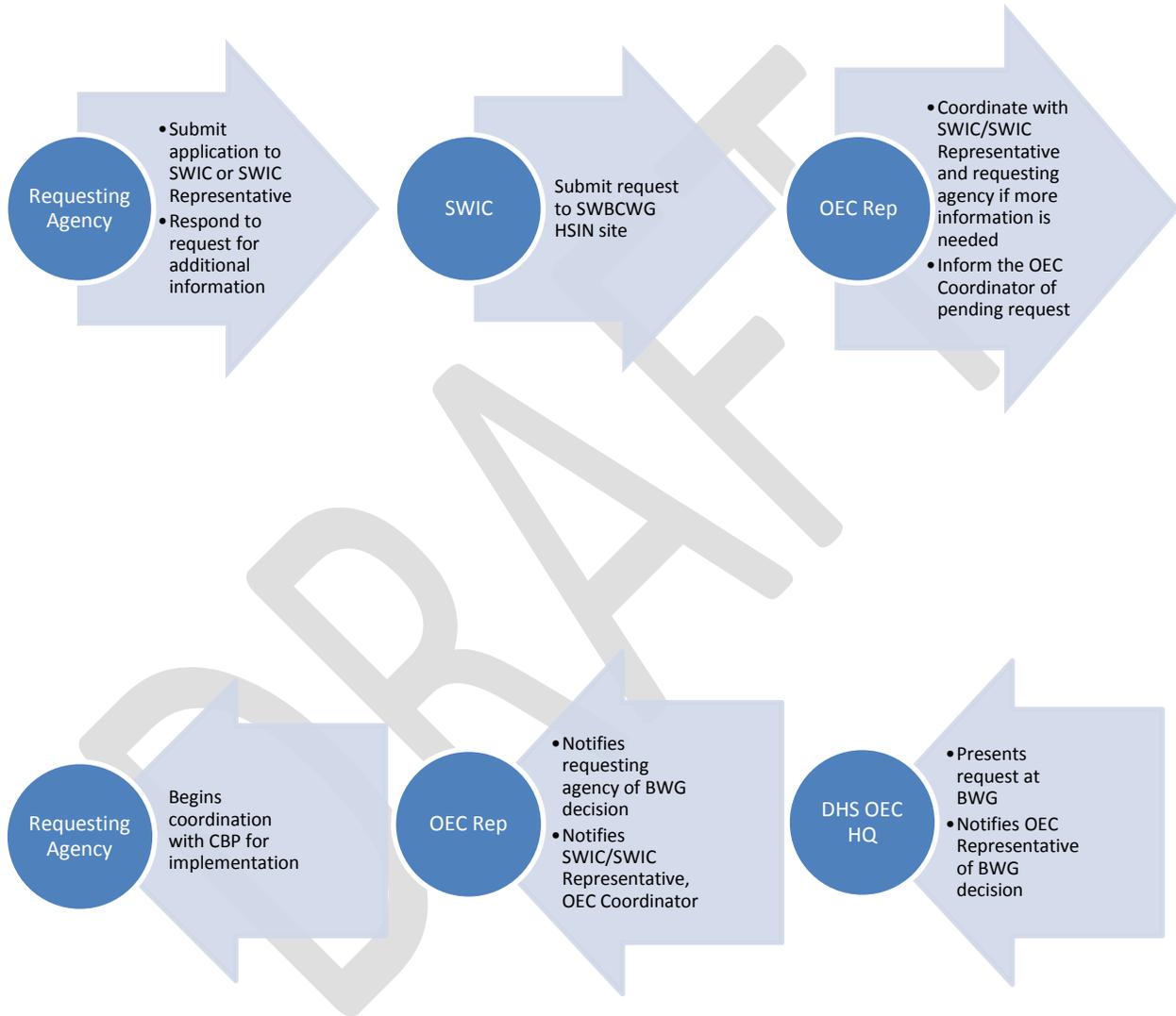


Figure 1: Process for submitting CBSCN access applications

SECTION III. BORDER/CROSS-BORDER NETWORK USAGE ELIGIBILITY

As stated in Appendix I.A, certain Federal, State, Local, Tribal and Public Security/Safety Organizations may be invited to interconnect their entities to the CBSCN. Examples of eligible agencies shall include:

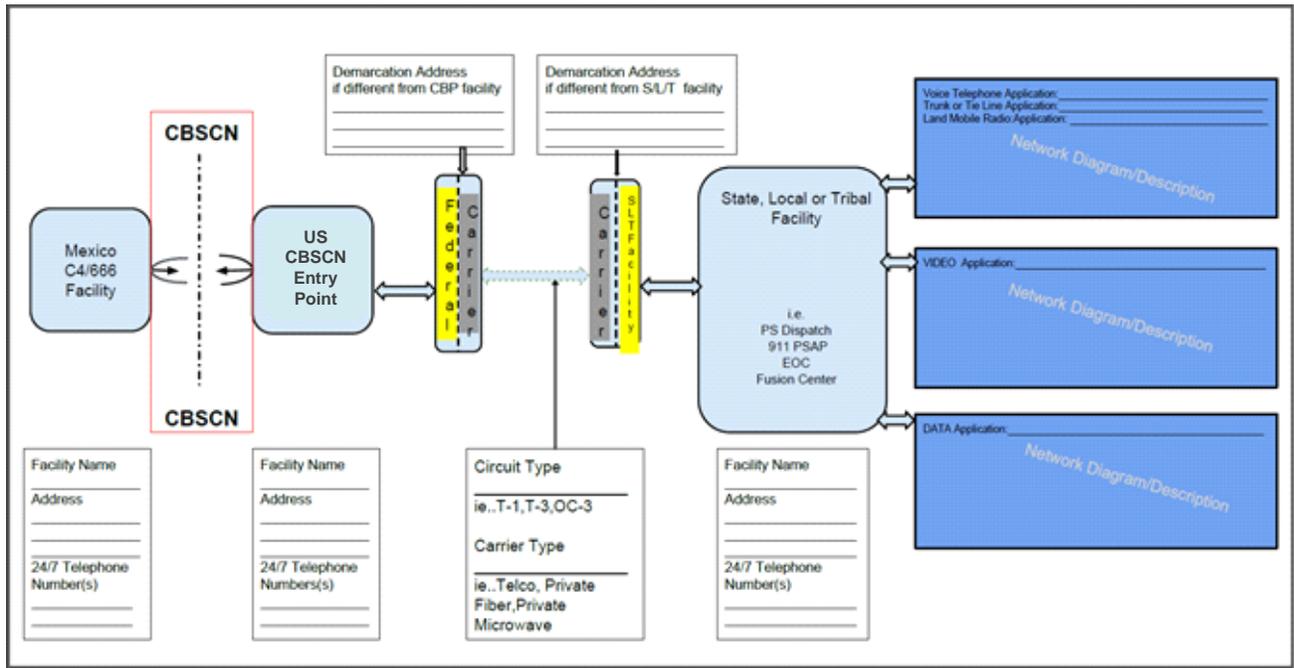
- **Law Enforcement:** Federal, State, local and tribal government law enforcement officials;
- **Fire Departments:** Command and other fire suppression and investigative personnel, responsible for directing fire emergencies at or near the shared border;
- **Emergency Medical Services (EMS):** Transport ground and air EMS resources that respond to emergencies at or near the shared border;
- **9-1-1 PSAPs/Public Safety Dispatch Centers:** Federal, State, local, and tribal dispatch centers that routinely deal with border emergencies and are legally licensed according to FCC rules to operate radio frequency resources;
- **Other Key Responders:** Emergency coordinators or officials that have border security responsibilities and are authorized on a case-by-case basis based on specific regional requirements. Public works and transportation agencies, working under direction of law enforcement, EMS or fire departments, are also eligible to use the CBSCN.

SECTION IV. IMPLEMENTATION PROCESS

Once the application is approved to move into the implementation phase, the OEC Representative(s) will notify the requesting agency. Once notified, agencies will:

- Identify Project Manager or team lead responsible for coordinating the effort
- Develop a project plan. The project plan must include but is not limited to the following:
 - To whom and where the agency plans to connect
 - A communications plan (to include POC information for US and Mexico, stakeholders, project sponsors, etc.)
 - Preliminary Network Design, Specifications and proposed applications/connections [complete diagram including locations, call signs, and other station identifiers, proposed network connections, data flows, applications, computing resources connected, etc.] (see sample diagram below)
 - The Features/functions that will be utilized.
 - Types and amount of data/communications that will transverse the network
 - Amount and Type of Encryption
 - Quality of Services (QoS) levels being requested
 - Preliminary Project Schedule
- Confirm/identify funding (initial and O&M/fee for service models)
- Develop and submit a SOP. The SOP must include but is not limited to:
 - In which circumstances connections will be made
 - How the connections will be made
 - How O&M will be addressed
- Submit Project Plan and supporting information to OEC Representative(s)
- OEC will submit documentation to the current Network & System Security Engineering Authorities

Figure 2: Sample Network Diagram / Preliminary Network Design



SECTION V. APPROVAL

- Finalized project plan will be submitted through established channels for approval by CBSCN Network Owner and Network Systems Security Engineering Authorities
- Decisions granting or denying access will be provided to the requesting agency through OEC
- If necessary, additional meetings can be held to discuss any decisions.

SECTION VI. AGREEMENTS

These procedures shall go into effect on the date signed by the Co-Chairs and govern the actions of affected US parties. Changes to this appendix must be submitted to and approved by the Co-Chairs.

SECTION VII. SIGNATURES

ENDORSED BY:

Signature	Signature
Date: _____, 2014	Date: _____, 2014

Ronald Hewitt, Director, Office of Emergency Communications Office of Cybersecurity & Communications National Protection and Programs Directorate	Robert Martin, Director, Wireless Systems Program Division Office of Information and Technology, U.S. Customs and Border Protection (CBP)
--	--

APPROVED BY:

Signature	Signature
Date: _____, 2014	Date: _____, 2014
Charles Armstrong, BWG Co-chair representing United States of America Assistant Commissioner and Chief Information Officer, Office of Information and Technology, U.S. Customs and Border Protection (CBP)	Ricardo Marquez Blas, BWG Co-chair representing United Mexican States National Security Commission, Secretariat of the Interior, (SEGOB)

DRAFT

CROSS BORDER SECURITY COMMUNICATIONS NETWORK (CBSCN) APPLICATION FOR NETWORK ACCESS

Information for United States Applicant				
Date of Application				Region
Name of Organization/Agency				
Organization/Agency Address				
City		State		ZIP
Name of Submitter				
OEC Representative for Organization				
SWIC POC (as applicable)				
Agency type				
<input type="checkbox"/> Law Enforcement	<input type="checkbox"/> Transportation	<input type="checkbox"/> National Guard or State Military Forces		
<input type="checkbox"/> Fire Department	<input type="checkbox"/> Non-Governmental (NGO) Support – Red Cross, Salvation Army, etc.	<input type="checkbox"/> Critical Infrastructure		
<input type="checkbox"/> Emergency Medical Services	<input type="checkbox"/> Weather Service	<input type="checkbox"/> 9-1-1/Public Safety Communications		
<input type="checkbox"/> Homeland Security	<input type="checkbox"/> Regulatory	<input type="checkbox"/> Local, Country, or State Governments		
<input type="checkbox"/> Other (Please Specify):				
Primary POC Information				
Name of Primary POC				
Primary POC's Title				
Primary POC's Email				
Name of Primary Technical POC				
Primary Technical POC's Title				
Primary Technical POC's Email				
Alternate POC Information				
Name of Alternate POC				
Alternate POC's Title				
Alternate POC's Email				
Name of Alternate Technical POC				
Alternate Technical POC's Title				
Alternate Technical POC's Email				

Scenario Details		
Which scenario(s) apply to your organization? (as stated in Appendix 1B) (Select all that apply)		
<input type="checkbox"/> Natural Disaster	<input type="checkbox"/> Transnational Criminal Activity	<input type="checkbox"/> Terror Threats
<input type="checkbox"/> Medical Emergency	<input type="checkbox"/> Hazardous Materials	<input type="checkbox"/> Border Violence
<input type="checkbox"/> Information Sharing/Missing	<input type="checkbox"/> Escape and Evasion	<input type="checkbox"/> Other(Please Specify):
Funding		
Which type of funding will your organization use?		
<input type="checkbox"/> Federal Grants	<input type="checkbox"/> Federal Program	<input type="checkbox"/> State Program
<input type="checkbox"/> Other (Please Specify):		
Type of Connection(s) Requested		
Which type of request is this? (Check all that apply)		
<input type="checkbox"/> Voice (LMR, Telephony)	<input type="checkbox"/> Data	<input type="checkbox"/> Video
Information for Mexican Organization		
Identify which Agencies/Organizations within Mexico you are wishing to connect to:		
Mexican Agency type		
<input type="checkbox"/> Law Enforcement	<input type="checkbox"/> Transportation	<input type="checkbox"/> National Guard or Military Forces
<input type="checkbox"/> Fire Department	<input type="checkbox"/> Non-Governmental (NGO) Support – Red Cross, Salvation Army, etc.	<input type="checkbox"/> Critical Infrastructure
<input type="checkbox"/> Emergency Medical Services	<input type="checkbox"/> Weather Service	<input type="checkbox"/> Other (Please Specify):
<input type="checkbox"/> Homeland Security	<input type="checkbox"/> Regulatory	
<input type="checkbox"/> 911/Public Safety Communications Center	<input type="checkbox"/> Local, Country, or State Governments	
Additional Details/Remarks		
Describe any additional details pertaining to this submission:		
	Date	