U.S. Department of Homeland Security

Office of Grants and Training

Tactical Interoperable Communications Plan Review Process

Homeland Security

March 2006

Tactical Interoperable Communications Plan (TICP)
Review Process

Introduction:

As part of the Department of Homeland Security (DHS) Fiscal Year 2005 Homeland Security Grant Program (HSGP) guidance, each Urban Area (UA) receiving Fiscal Year 2005 Urban Area Security Initiative funds must develop a plan to achieve tactical interoperable communications across all jurisdictions in the UA and test the plan through a full-scale exercise. Each State that does not have a designated UA must name a multi-jurisdictional metropolitan area or region to meet the tactical interoperable communications requirements of the Fiscal Year 2005 program.

The following is a summary of the review process that the Office of Grants and Training (G&T) will use in evaluating the Tactical Interoperable Communications Plan (TICP). This review process is designed to make grantees aware of their successful completion or any deficiencies within their plans. Grantees will also be advised of next steps according to the outcome of the TICP review.

I. Purpose & Scope:

To help with the TICP review, the Interoperable Communications Technical Assistance Program (ICTAP) has developed a TICP Review Checklist that will be referenced during the process. This checklist has been derived from the Fiscal Year 2005 HSGP guidance requirement and will determine if the TICPs are:

- Focused on grant guidance requirements
- Producing uniform, standardized results
- Meeting expectations concerning capabilities-based planning
- Providing a baseline for understanding a site's status and interoperable communications needs
- Providing feedback to sites
- Providing feedback to G&T

In addition, the checklist will serve as a guide for validation of the tactical interoperable communications during a live field exercise.

II. Capabilities-Based Planning:

As detailed in G&T Information Bulletin 192 released on October 14, 2005:

"The release of the National Preparedness Goal, Target Capabilities List (TCL), and Universal Task List (UTL) presents an opportunity to build a foundation of capabilities-based

planning. The TCL: Version 2.2 represents a significant step forward in developing those readiness targets. It identifies 37 capabilities required to prevent, protect against, respond to, and recover from incidents of national significance. As jurisdictions plan their exercises, the Interoperable Communications Target Capability and "designated" Critical Tasks must be incorporated into their exercise activity to test the TICP."

Each TICP will be reviewed against the performance measures associated with the Interoperable Communications Target Capability. As the performance measures have varying degrees of applicability to the TICP, sites have been given a checklist (see Attachment 1) detailing the TICP requirements.

III. TICP Submittal Process:

Copies of the TICP must be submitted by the State Administrative Agency (SAA) to the G&T Preparedness Officer via the ODP Secure Portal. A designated "TICP" submittal area has been setup for reference. For those who do not have a current account, you will have to register by invitation. Instructions on how to register and log on to the ODP Secure Portal are provided in Attachment 3. These materials will then be made available to the ICTAP Program Manager (PM) to begin the review process.

IV. Peer Review Panel:

A peer review panel will be utilized for the TICP evaluation process. Selected individuals from the local, State and Federal public safety/first responder community will be assigned as panel members and will review the TICPs independently before providing recommendations during a two-day panel session convened at DHS headquarters. These panel sessions will be scheduled as needed. The reviewers will receive a copy of the TICP via CD-ROM and/or the ODP Secure Portal prior to the panel convening.

When convened, the panel will evaluate the TICP, using the TICP Review Checklist, and provide a review decision. This is a subjective process based on the content of each TICP. These TICPs are "For Official Use Only" and contain highly sensitive homeland security information; therefore, TICPs shall not be reproduced or shared beyond the panel members. Each panel member will be requested to execute a conflict of interest agreement that he/she has no direct relationship to a specific TICP and to sign a nondisclosure agreement.

V. TICP Review:

Each member of the panel will complete a separate TICP Review Worksheet (see Attachment 2). Upon the completion of the review session, panel members must come to a consensus whether the plan meets one of two categories: "pass" or "need additional information". In the event that peer review panel members cannot reach a consensus on the evaluation of a TICP, the Director of the Preparedness Programs Division will make the final determination. The panel's overall evaluation will be noted on page 1 of the Worksheet under "Panel Review Record."

In the event a TICP has been evaluated to "need additional information," the SAA, TICP site, and Preparedness Officer (PO) will be informed of the decision. Grantees will be given a prescribed time frame to submit "only" the requested information. The TICP review process

cannot be successfully completed until the information has been received and approved by G&T. The TICP review process will take up to 45 days from the submittal date.

VI. Composition of the Peer Review Panel:

The peer review panels will consist of five to seven representatives from local, State, and Federal agencies and from relevant National Associations. In addition, the ICTAP PM will serve as chairman, recorder, and facilitator of each panel. A senior manager from G&T will serve as an observer for each panel. The ICTAP PM and G&T Preparedness Officers will not serve as a peer reviewers.

Below is a list of possible agencies and associations from which individuals will be selected to participate as a review panelist:

A. Federal Agencies

- **Department of Homeland Security**
  - Office of Grants and Training (G&T)
  - SAFECOM
  - Wireless Management Office (WMO)
  - National Incident Management System Integration Center (NIMS/NIC)
  - Federal Emergency Management Agency (FEMA)
- **Department of Justice**
  - National Institute of Justice-Communications Technologies (NIJ-CommTech)
  - Department of Justice-Community Oriented Police Services (DOJ-COPS)
  - Federal Bureau of Investigation (FBI)
- **Federal Communications Commission (FCC)**
- **National Guard Bureau**

B. National Associations

- National Sheriffs Association (NSA)
- Major Cities Chiefs Association (MCC)
- International Association of Chiefs of Police (IACP)
- International Association of Fire Chiefs (IAFC)
- US Conference of Mayors (USCM)
- National Governors Association (NGA)
- National Public Safety Telecommunications Council (NPSTC)
- Association of Public Safety Communications Officials International (APCO)
- National Association of State EMS Directors (NASEMSD)
- National Association of Telecommunications Officers and Advisors (NATO
- National Emergency Management Association (NEMA)
- National Emergency Number Association (NENA)
- National Public Safety Telecommunications Council (NPSTC)

VII. Decision Package to G&T Management:

Upon completion of a peer review panel, a formal decision package will be submitted to G&T management for review and approval. This package will include:

- A routing memo from the ICTAP PM (through the Preparedness Programs Division) to the responsible Preparedness Officer
- Hard copies of completed TICP Review Checklist
- A hard copy of the subject TICP
- A status letter to be signed by the G&T Technical Assistance Division Director informing the TICP site of the TICP Review results

All completed documentation will be provided to the designated Preparedness Officer by ICTAP Support following the results of the peer review panel.

VIII. Notification of Review Results:

Upon receiving the formal decision package with all necessary signatures/initials, the responsible Preparedness Officer shall:

- Send the status letter (signed by the G&T Technical Assistance Division Director) informing the TICP site of the review results. Attached will be a summarized overview of the checklist results. The letter should include a copy to any SAA POCs that the Preparedness Officer feels should be notified regarding the TICP review.

- Inform all appropriate G&T personnel via email of the review results. The Preparedness Officer must notify the Director of Preparedness Programs, the Director of the Exercise and Evaluation Division, the Director of the Training Division, the G&T Legislative Affairs staff, and Centralized Scheduling and Information Desk.

If there are any questions regarding the results of the review or decision packet, please feel free to contact your G&T Preparedness Officer and/or the ICTAP Program Manager, Keith Young, keith.young@dhs.gov.

IX. Attachments:

Attachment 1: Common Capabilities: Interoperable Communications Performance Measures and Objectives
Attachment 2: TICP Review Worksheets
Attachment 3: Instructions for submitting TICP on the ODP Secure Portal

Attachment 1:
Common Capabilities: Interoperable Communications Performance Measures and Objectives

Common Capabilities: Interoperable Communications Performance Measures and Objectives			
Performance Measure	**TICP Implication**	**TICP Reference**	**TICP Site Notes**
A multi-agency and multi-jurisdictional governance structure is in place to improve communications interoperability planning and coordination.	***The TICP must document a multi-jurisdictional governance structure***		
Participating entities in the governance structure have developed and will update interoperability communications plans as needed.	***The TICP should document how the governance group will maintain the plan and ensure that agency information is current***		
Formal agreements exist among jurisdictions and disciplines.	***While not a requirement of the TICP, any multi-jurisdictional plan should be supported by mutual aid agreements and/or regional MOAs/MOUs***		
Governance committees have developed a plan to acquire and influence sustained interoperability and systems maintenance funding.	***Not a requirement of the TICP***		
A regional set of communications Standard Operating Procedures (SOPs) that conform to NIMS are in place and implemented and include operational and technical elements.	***Communications policies and procedures must be documented in the TICP***		
Command and control policies are in place to achieve interoperability as necessary.	***The TICP must detail communications command and control procedures.***		
Interoperability policies and procedures are in place to allow information sharing between levels of government and federal installations involved in the incident as necessary.	***The TICP must include all public safety agencies within the UAWG, and sites are encouraged to include additional Federal, State and local agencies***		
Individual agencies across the jurisdictions have operable communications systems in place.	***The TICP must document the voice interoperable communications equipment inventory of all participating agencies.***		
Appropriate levels of redundant communication systems are available.	***It is recommended that the TICP incident communications plan (Section 5) include backup interoperability methods to be used***		

All personnel are trained to operate communications systems according to their role at an incident.	***The TICP should identify individuals to receive the NIMS Communications Unit Leader training currently under development by SAFECOM***		
Plans, procedures, and use of interoperable communications equipment have been exercised.	***The TICP must be validated through a full scale, multi-jurisdictional exercise by the Urban Area***		
Interoperability systems are used in pertinent everyday activities as well as emergency incidents to ensure users are familiar with the system and routinely work in concert with one another.	***Sites are encouraged to utilize the interoperability methods detailed in your TICP to ensure proper use in an emergency.***		
An assessment of standard communication capabilities for the PSAPs/Public Safety Communication Centers, and Emergency Operations Centers (EOC), has been completed to ensure an appropriate continuity of operations plan (COOP) is in place for public safety and service agencies' communications.	***Not a requirement of the TICP***		
A common operating picture (COP) for real time sharing of information with all the participating entities can be established as required.	***While not a requirement of the TICP, the Communications Asset Survey and Mapping tool (CASM) offered through the ICTAP program provides a regional communications picture to users.***		

Attachment 2:
TICP Review Worksheets

This is a worksheet for use by peer review panel members for evaluation of all Tactical Interoperable Communications Plans

Tactical Interoperable Communications Plan (TICP) Approval Review Checklist

TICP Site: _____ _____

G&T Preparedness Officer: _____

ICTAP PM Recording Secretary: _____

Overall Result (circle one): PASS

NEED ADDITIONAL INFORMATION

Date of Panel Meeting: _____

Reviewer: _____ Reviewer's Organization: _____

Part I: Strengthen Interoperable Communications Capabilities

As indicated in Fiscal Year 2005 and Fiscal Year 2006 Homeland Security Grant Program guidance tactical interoperable communications is seen as a key capability supporting Homeland Security strategic goals and national priorities. The following questions about the TICP under review are based on Homeland Security Presidential Directive-8, Information Bulletin 192, "Tactical Interoperable Communications Plan (TICP) Exercise Guidance," and the DHS SAFECOM Interoperability Continuum.

OVERALL TICP EVALUATION FINDINGS

1. How well does the TICP establish a plan to achieve tactical interoperable communications across jurisdictions in the region?

2. How well does this TICP support long-term interoperability?

3. How well does the TICP incorporate the Interoperable Communications Target Capability performance measures (See accompanying chart for more information)?

TICP Acceptance Checklist

Pass	Need Add. Information	Element	Comments
TICP Requirements (bulleted items are recommended but not required)			
		1. Urban Area Information	
☐	☐	1.1. Provides an overview of the area consistent with the Urban Area or State Homeland Security Strategy	
☐	☐	1.2. Lists all included agencies	
☐	☐	1.3. Notes the plan's point of contact	
		2. Governance	
☐	☐	2.1. Provides an overview of the governance structure that will oversee and implement the plan	
		• Establishes responsibilities of the governing body and sub-groups	
		• Provides a meeting schedule for the governing body	
		• Describes individual agency responsibilities and rights	
		• States regional authority for coordination and assignment of assets	
		• Establishes a working group responsible for determining operational requirements, developing Standard Operating Procedures, and coordinating training	

Pass	Need Add. Information	Element	Comments
		• Establishes a working group responsible for identifying, developing, and overseeing technical solutions	
☐	☐	2.2 Lists participants, agencies represented, and roles	
		3. Interoperability Equipment	
☐	☐	3.1 Lists resources to be used and the responsible agency(s) for operation and maintenance through swapping radios (if applicable)	
☐	☐	3.2 Lists resources to be used and the responsible agency(s) for operation and maintenance through sharing channels (if applicable)	
☐	☐	3.3 Lists resources to be used and the responsible agency(s) for operation and maintenance through gateways (if applicable)	
☐	☐	3.4 Lists resources to be used and the responsible agency(s) for operation and maintenance through shared systems (if applicable)	
		4. Policies & Procedures	
☐	☐	4.1 Establishes policies and procedures for **swapping radios** (if applicable)	
		• Participating agencies list	
		• Best practices	
		• Rules of use	
		• Request procedures	

Pass	Need Add. Information	Element	Comments
		• Activation procedures	
		• Deactivation procedures	
☐	☐	4.2 Establishes policies and procedures for other **shared channels** (if applicable)	
		• Participating agencies list	
		• Best practices	
		• Rules of use	
		• Usage procedures	
		• Problem identification and resolution procedures	
☐	☐	4.3 Establishes policies and procedures for **gateways** (if applicable)	
		• Participating agencies list	
		• Best practices	
		• Rules of use	
		• Request procedures	
		• Activation procedures	
		• Deactivation procedures	

Pass	Need Add. Information	Element	Comments
		• Problem identification and resolution procedures	
☐	☐	4.4 Establishes policies and procedures for **shared systems (if applicable)**	
		• Participating agencies list	
		• Best practices	
		• Rules of use	
		• Problem identification and resolution procedures	
		5. Plans for Tactical Communications During an Incident	
☐	☐	5.1 Documents participating functional disciplines	
☐	☐	5.2 Describes how communications resources will support the incident management system and command structure	
☐	☐	5.3 Establishes the methods of communication for Incident command and general staff	
		• Operations Section (including any functional groups or geographic divisions)	
		• Planning Section	
		• Logistics Section	
		• Finance/Administration (if established)	

Pass	Need Add. Information	Element	Comments
		6. Training	
☐	☐	6.1 Ensures that sufficient personnel are trained as Communications Unit Leaders as defined within NIMS	
☐	☐	6.2 Documents the number of certified Communications Unit Leaders and disciplines which they serve	
☐	☐	6.3 Ensures that trained Communications Unit Leaders are available at all times	

Attachment 3:

Instructions for submitting TICP on the ODP Secure Portal

In order to gain access to the ODP Secure Portal please email your name and contact information to Ralph Barnett at Ralph.Barnett@associates.dhs.gov and Matthew Biancucci at Matthew.Biancucci@associates.dhs.gov . Upon receipt of your e-mail, you will be sent an invitation to register. Once the registration process is complete, your account will be approved and you will be able to logon to the system.

The three tools that will be most widely utilized through this process are the Library, Secure Messaging and Chat. Please follow the steps below in order to use these tools. Should you have any questions regarding the registration process or how to upload a document please contact Sarah Greider at (703) 682-6019, sgreider@espgroup.net or the Help Desk at (804) 744-8800, helpdesk@espgroup.net

Library
This tool allows you to upload and share documents with other users:

- Click on the "Collaboration" link from the desktop.
- Select the "Library" link from the list of collaboration tools.
- Click on the appropriate folder listed in the left hand frame (all folders will follow the same scheme as "TICP – State/Urban Area")
- Once you have selected the folder, click the "Upload Document" link in the middle of the folder screen on the right hand side.
- Type in a file name, a brief document description and select the file from your computer to upload. Click the "Finished" button to upload your file.

Secure Messaging
This tool allows you to send internal messages, with attachments, to any other user participating in the ODP Secure Portal:

- Click on the "Collaboration" link from the desktop.
- Select the "Secure Messaging" link from the list of collaboration tools.
- Click on "Compose Message" in the upper right hand side.
- Use the search feature to send a message to an organization or another portal user (make sure the appropriate "Orgs" or "Users" box is checked when searching.)
- Highlight the organization name and click the "To" box to move the name into the "To:" column.
- Type in a subject and message.
- Select a notification option at the bottom.
- Click "Send" to send the message.

Chat
This tool allows users to participate in a real-time chat with other users participating in the system. Use this tool to post questions regarding the program and/or the ODP Secure Portal:

- Click on the "Collaboration" link from the desktop.
- Click on the "Chat" link from the list of collaboration tools.
- Select the "Questions and Answers Chat" from the drop down box in order to join the discussion.
- Use the text box in the bottom right hand corner to post a message. If you post a question in this area, you will receive a written response from an Administrator within 48 hours of your posting
- Use the "View Transcript" hyperlink in the upper right hand corner to view previous chat postings.