



Team Awareness Kit (TAK) -

Enhancing Homeland Security Enterprise Collaboration
on the Mobile Edge

A Whitepaper by DHS S&T

December 2019



**Homeland
Security**

Science and Technology

Situational awareness technology transforming from the battle zones to the front lines of DHS Components and Public Safety Agencies

The Team Awareness Kit (TAK) provides real-time access and collaboration channels to organizations within the Homeland Security Enterprise in various cost models.

What TAK Provides

When we think of situational awareness for the Department of Homeland Security (DHS) team operators, we often think of split second delivery of information and life saving alerts to inform those who help protect us in an emergency. TAK is one of those breakthroughs in technology. Developed by the Air Force Research Laboratory (Rome, NY), TAK enables situational awareness and collaboration in real time (see Fig. 1) for team members situated in the field and at command centers.

Over the past five years, DHS Science and Technology Directorate (S&T) has successfully leveraged this system to support federal agency response during natural disasters and coordinated operations.

How TAK Can be Obtained/Deployed

TAK consists of server and client (e.g., mobile app) software, which is free for government and public safety use, but requires hardware to run on (server, mobile device, etc.) and technical support to install and maintain the software. Based on the existing hardware/technical support that they already have, organizations can determine which TAK option reflects the best cost model for their implementation.

S&T offers this white paper to inform all potential interested parties, including federal, state, local and tribal agencies about TAK, what it does, the benefits, and resources to help with licensing, setup and support for the tool.



Real-time Situational Awareness between field ops and command center

Fig. 1 TAK deployment.

Options for Implementing TAK

TAK is Government off-the-shelf software that is free of charge for government and public safety organizations, but requires resources (e.g., people and hardware) to effectively incorporate it into an operational system. For some (usually larger) organizations, those resources are already available; for other (usually smaller) organizations, those resources may be unavailable.

Based on their situations, individual organizations can select one of the following general models for implementing TAK:

- **In-House Model:** Organizations with a robust set of existing hardware, information technology (IT) departments, and trainers may opt to obtain the TAK software and have those existing resources deploy and maintain the TAK software.
 - **Commercial Model:** Organizations with minimal in-house IT infrastructure and expertise may opt to pay a service fee to a vendor to manage the TAK implementation for them.
 - **Bring Your Own Device (BYOD):** The FBI is initiating a program to provide public safety organizations with access to a TAK server for use with their own devices, with TAK clients (e.g., mobile app) already installed.
- **IT Resources:** Organizations have various "sunk costs" in IT infrastructure and IT personnel with some organizations able to support TAK implementation by leveraging existing resources, while other organizations would need to make new investments in those areas specifically for TAK.
 - **Training Resources:** Organizations need personnel to develop practical guidance for using the TAK software and to train people on how to effectively deploy TAK to support mission-critical operations.
 - **Data Sensitivity:** Organizations have various sensitivities related to their data (law enforcement, disaster response, etc.) and associated cyber-security requirements to protect the data (e.g., security accreditation for TAK servers).
 - **Cross-Organizational Collaboration:** Government agencies and public safety organizations often coordinate during ongoing operations and specific events (or incidents) and share information as part of those collaborations.

Considerations for Implementation Model Selection

There are many factors to consider when selecting a TAK implementation model and these factors have different weights among different organizations. A sample of the key factors follows below.



TAK—a Snapshot

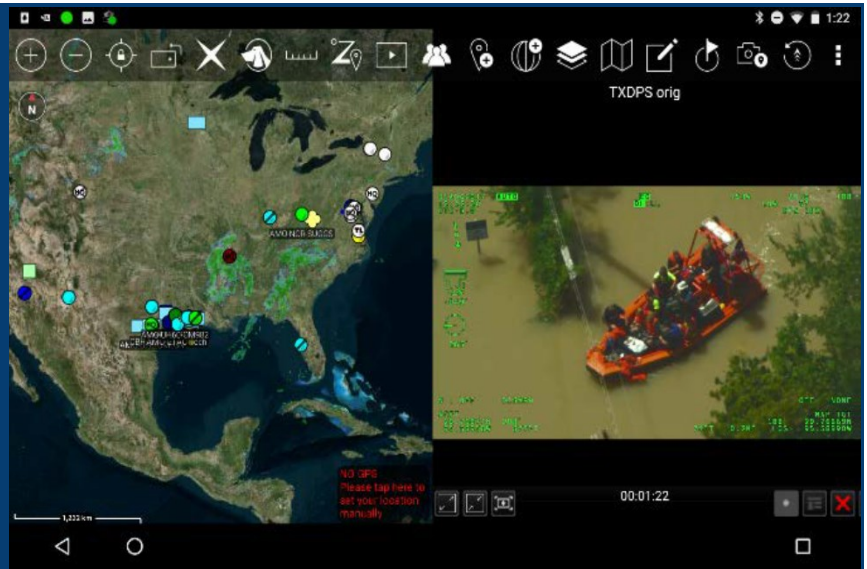
In August of 2017, Hurricane Harvey ripped through the state of Texas. The federal, state, and local response was massive. The DHS S&T deployed the Android Team Awareness Kit (ATAK) to support the complex communication and coordination needs of the multi jurisdictional responders.

ATAK dramatically alters the user's understanding of the action in any given area of operation. These users, known as "operators," could be law enforcement, fire, emergency medical service, personnel from other agencies, or even military. Instead of hearing intermittent radio transmissions from unknown operators at unknown locations while simultaneously engaging in an action themselves, these operators can now see who and where those elements are on a mobile screen, and even communicate with team members from different agencies, and do it in a multitude of ways.

Most of the operators with ATAK in Texas had never used it before and many were skeptical. However, the ease of use, situational awareness, and cross agency communication and coordination capabilities of ATAK quickly won them over. Multiple organizations used it to coordinate rescues, respond to criminal activity, identify infrastructure breaches, and establish perimeters in danger zones, in addition to multiple other collaborative activities.

TSgt Kyle Evans, with the 147th ASOS TACP/JTAC of the Texas Air National Guard, was part of the Hurricane Harvey Joint Air Ground Control Team. He said that ATAK, "started on our end as a way to track my guys in the field. Over the past days, use has blown up." The stunning situational awareness and ability to react in real time has operators like TSgt Evans wanting their HQs to incorporate it enterprise wide because with ATAK, "I can move faster... way faster than they can."

The success of ATAK in Texas prompted it to be deployed when Florida was slammed by Hurricane Irma. Again, ATAK proved its worth in a crisis.



TAK—FAQ’s for Evaluating Implementation Options

What is the Difference in TAK Clients? The TAK server (software) can interface with one or more TAK client (software), which is associated with different end user devices (see Fig. 2). The interface between the TAK server (software) and TAK client (software) is the same, and multiple different TAK clients can all interface with the same TAK server at the same time.

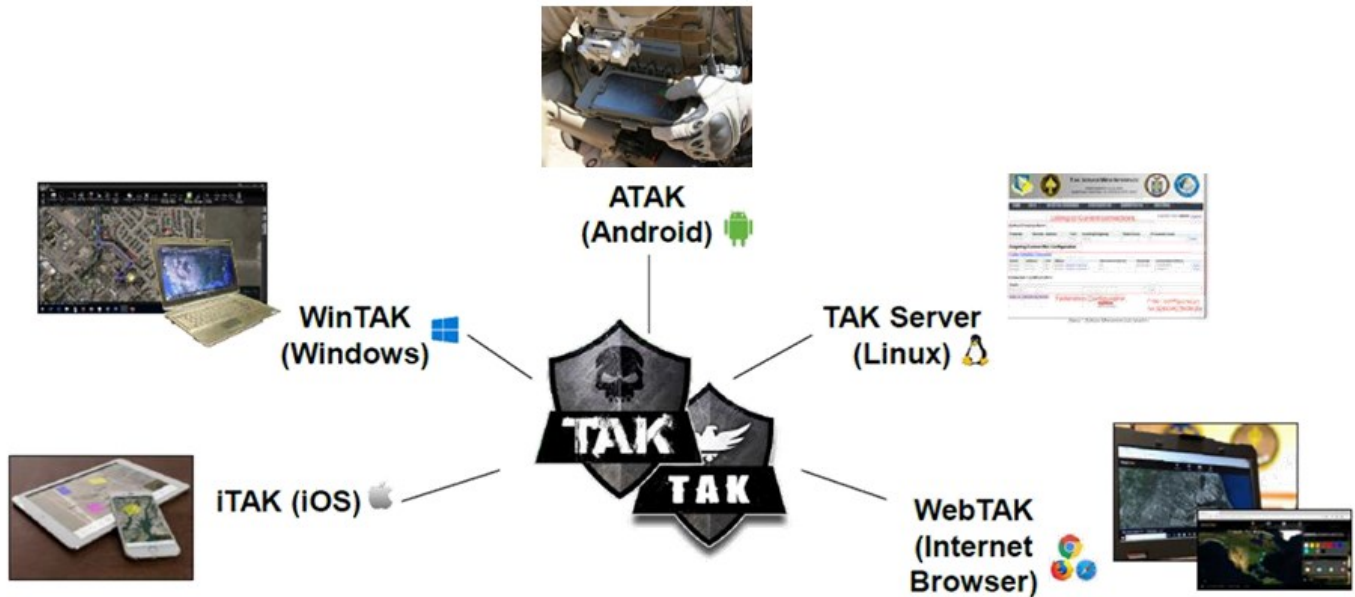


Fig. 2 TAK server and clients.

Android Team Awareness Kit (ATAK): A mobile app that can be installed on Android mobile devices, which was the original TAK client developed and has the most robust features of all TAK clients based on size and length of development investment. In addition, Android (and hence, ATAK) is built on an open architecture which allows "plug-ins" to be developed to extend the ATAK core functionality to support additional (organizational specific) functionality such as communication device support, data exchange interface to a non-TAK server, or operational capability.

Windows Team Awareness Kit (WinTAK): An application that can be installed on Windows devices (e.g. computer), which was developed to enable personnel in command centers to exchange data with users in the field (using ATAK) on the infrastructure already employed in the command center. WinTAK software mimics most functionality in ATAK but the software itself was written from scratch for Windows (rather than Android) and there are some differences in the interface and functionality.

iOS (i.e. iPhone) Team Awareness Kit (iTAK): A mobile app that can be installed on iOS devices (i.e. iPhone and iPads), which is currently under development, will be launched after a successful beta prototype. Like WinTAK, iTAK software itself is being written from scratch to mimic functionality in ATAK, but the beta prototype and even the initial operationally ready version will have a subset of the most used functionality found in ATAK.

Web Team Awareness Kit (WebTAK): A web-based interface which allows users to type in the website for a specific TAK server (configured to support WebTAK) was recently developed. The primary use of WebTAK is to provide quick access to data collected in the TAK server to enable situational awareness to be shared and avoid having to install TAK clients (i.e. ATAK, WinTAK, iTAK) on hardware.

TAK—FAQ's For Evaluating Implementation Options (con't)

Does TAK Solve "Comms" Issues? TAK clients use the native communications built into the hardware (e.g. cellular, wi-fi, etc.) to pass data across an existing network to the TAK server (and onto other devices with TAK clients). ATAK supports a "plug-in" architecture, which allows non-native communications provided by external communications devices (e.g. SATCOM, MANET, etc.), to interface with ATAK and pass data across the networks created by those external communication devices. This allows ATAK to be used with technologies which solve some of the current "comms" issues encountered by end users.

How Do I Get the TAK Software for an "In House" Implementation? The joint TAK program office has a public website that people can access and send in requests for the TAK software (and other inquiries), which then go through their vetting process to ensure proper distribution and use of the TAK software. To contact the TAK program office visit <https://takmaps.com/>.

How Do I Go About Soliciting and Selecting a Commercial Vendor for TAK Services? DHS S&T recommends that each agency assess its own requirements and have an established checklist ready to ensure the commercial vendor's TAK solution meets the availability and technical support needs of your agency.

How Do I Get More Information about the "BYOD" FBI TAK Program? The FBI is providing TAK support to include TAK server access through its existing Law Enforcement Enterprise Portal (LEEP) program. A pilot was conducted during Fiscal Year (FY) 2019 and is fully operational in FY2020. To contact the FBI regarding TAK visit <https://www.fbi.gov/services/cjis/leep>.

What are the IT Resource Requirements for TAK? The TAK server requires server hardware along with someone to install and maintain the software. The TAK clients require some sort of hardware (e.g. mobile device or computer) that can be installed on existing hardware or other applications, and will need someone to install and maintain the software. The TAK client also needs a network to communicate over, which can be existing/expanded cellular service on a mobile device the TAK client is installed on, or another network solution.

What are the TAK Training Requirements? TAK client training for basic "button-ology" is fairly simple and a series of short instructional videos was developed by DHS S&T to quickly do remote training for disparate responders to Hurricane Harvey, which enabled them to effectively use TAK. More advanced and administration training is available using existing TAK materials. One training area that needs to be addressed locally is how to use TAK in local operations such as how to provide updates (e.g. symbols to use and naming conventions), how to respond to those updates (e.g. all end users rush to update or just closest end user), and other standard operating procedure considerations so everyone uses TAK in the same way within an organization.

What Data Sensitivity Considerations are there for TAK? While protecting all data is always of paramount importance, some data requires a defined level of security and/or certification technology. TAK servers maintained by federal organizations meet the level of security defined for the data and its availability. Commercial hosting of TAK servers may provide the same security measures but usually do not go through an official certification process. TAK clients may have various security measures put in place to include Mobile Device Management solutions that help to secure and manage overall configuration of mobile devices, which are employed by many federal and commercial organizations to manage their mobile devices at an enterprise level.

What Cross-Organizational Collaboration Considerations are there for TAK? Many government and public safety organizations work together for ongoing daily operations, (pre-planned) events, and (unplanned) incidents. To effectively coordinate and collaborate, these organizations need a way to share information and TAK has the ability to share data between TAK servers. Security measures such as firewalls meant to protect server environments from the larger networks they are connected to, may be a hurdle (but not an insurmountable one) for sharing data across TAK servers hosted in different server environments (e.g. FBI TAK server and Commercial Vendor TAK server). When determining which implementation model to select, an organization may want to inquire and/or coordinate with other organizations it collaborates with on the model they have or will select.