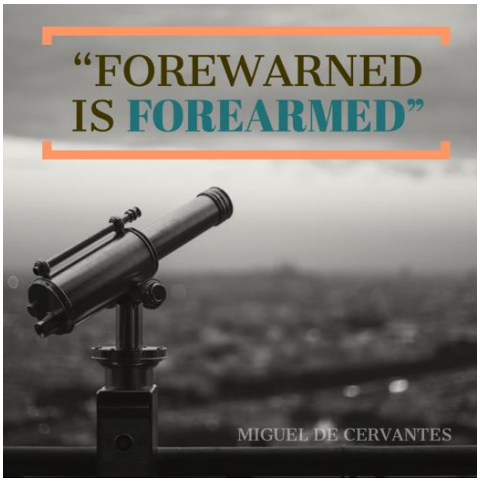
Duty to Warn Q & A

Making Sense of the Threat

Overview

From 2017 to 2019, several hundred U.S. private-sector organizations received phone calls from OSAC staff warning them of threats of killing, serious bodily injury, kidnapping, or physical attack directed at their organization's personnel and assets overseas. These alerts are referred to as *Duty to Warn (DTW) notifications*. In perspective, recipients of these calls represent a very small percentage of OSAC members and U.S. organizations. Consequently, these alerts are often the first of their kind for the recipient organization. This report seeks to clarify which circumstances spur a DTW notification, lay out simple steps U.S. and overseas security managers can take to be prepared to respond swiftly and measuredly if they become the target of a specific and credible threat, answer common questions, and describe what sort of follow-up to anticipate from OSAC and the U.S. Department of State.

Duty to what?



Security managers must regularly make decisions, allocate resources, and set decision points and tripwires based on assessments of events and trends that make up the threat environment in a given locale. These decisions account for risk, but rarely are they afforded the opportunity to factor in advanced knowledge of nefarious plotting. Armed with such knowledge when available, security managers can take additional measures to request support from local security personnel, augment internal countermeasures and procedures, adjust travel plans, or remove personnel altogether. OSAC has documented cases where this sort of information has verifiably prevented the loss of life. The goal of a DTW notification is to inform "left of bang" decision-making.

DTW obligates agencies of the U.S. Intelligence Community (IC) and the U.S. Government writ large to provide warning of known impending threats to specific individuals or groups. Intelligence Community Directive (ICD) 191, which governs the IC's DTW procedures, outlines a common understanding of the requirement.

Procedures and thresholds for sharing this type of information ultimately vary; however, with limited exceptions, agencies must always adhere to this requirement.

U.S. Department of State personnel handle the delivery of most DTW notifications involving private U.S. citizens and organizations overseas that result from specific, credible, and non-counterable threat information. The OSAC Global Threat Warning (GTW) team coordinates with Regional Security Officers (RSOs) at U.S. diplomatic posts abroad to perform these notifications in cases where U.S.-based companies, NGOs, faith-based organizations, and/or academia are the target of a threat. This duty covers OSAC members and non-members alike.

Specific, credible, and non-counterable?

These three thresholds form the basis of both the U.S. Department of State's DTW and its broader No Double Standard policy (NDS), which undergirds the Bureau of Consular Affairs Travel Advisory and Security Alert systems.

Requiring information to meet each of these thresholds accomplishes three important functions: it protects sources and methods by minimizing the unnecessary release of sensitive information; it avoids message fatigue resulting from oversharing of information that holds little value for the recipient; and it protects the integrity of the notifications that do occur.

When a member of the private sector receives a DTW notification, they can be confident that the underlying information has been determined to contain the following characteristics:

1. Sufficient detail to identify the specific target of a threat, plus enough information about the nature of the threat to inform mitigating action (**Specific**);
2. Has not demonstrated significant reason to doubt the credibility or reliability of the source (**Credible**);
3. Has not otherwise been shared with either the targeted organization or local security forces in such a way as to reasonably guarantee the disruption of the threat (**Non-Counterable**).

While these criteria are, by nature, subjective and fluid based on the circumstances of a given threat, they are never evaluated on an individual basis. Rather, OSAC consults with partner intelligence offices, agencies, and RSO shops to make these determinations.

How does OSAC acquire this information?

OSAC GTW is dedicated to performing threat watch functions, monitoring all-source reporting for information that meets the stated criteria, and engaging with relevant interagency partners to secure the release of a version of the information. This release is coordinated to strike a balance between protection of sensitive sources and methods and providing sufficient information to prove useful to security managers.

How does OSAC decide who to notify?

Closely tied to the specificity criteria is OSAC's policy that in order to trigger a DTW requirement, threat information must identify the targeted organization by name. In the event of such information, OSAC will notify only the named organization. There are rare exceptions to this rule, in which no organization is named, but OSAC knows a specific organization to be the only one operating in a named locale. If such a determination cannot be made, OSAC will defer to the Bureau of Consular Affairs for broad public messaging consideration. This approach avoids the possibility of notifying the "known" organization, while leaving in the dark other organizations unknown to OSAC. If the named organization is an OSAC member, OSAC staff will call the headquarters contact on file, while the RSO in the relevant country attempts to reach local security representatives for the organization. If the organization has no history with OSAC, staff will use whatever contact information is publicly available for the organization.

If I know of other U.S. organizations that may be impacted, can I share with them?

OSAC DTW notifications are unclassified, but are provided with handling instructions that discourage further sharing beyond personnel of the receiving organization who have a need to know. Limiting unnecessary dissemination of the information prevents confusion, circular reporting, and possible compromise of sources and methods. The U.S. Government has no recourse against organizations who decide to share the information further, and will never intentionally withhold future information because of mishandling. However, security managers should be aware of the implications that unapproved sharing may have on the USG's future ability to acquire and share similar information. Security managers who may have knowledge of additional affected organizations should consult with OSAC staff before sharing.

Is there any additional information?

The information that OSAC shares is the extent of what is available at that time. OSAC makes every effort to provide as many details as possible when sharing threat information. If the notification lacks substance, it is usually a reflection of the level of specificity in the original reporting. OSAC will provide additional notifications if relevant information becomes available.

Additionally, OSAC's regional analysts are always ready to discuss relevant trends and atmospherics. After receiving a DTW notification, you will be connected with the appropriate analyst who will be available for consultations to discuss the overall threat environment.

OSAC encourages feedback regarding the usefulness of a piece of information or the types of details that might have made the notification more impactful.

This warning is light on detail. Can you help me read between the lines?

While OSAC personnel are unable to comment further on details provided in a DTW notification, there are a few commonly recurring words and phrases whose meaning it can be helpful to understand. Here are a couple of tips for interpreting an alert:

1. Terminology is chosen carefully. In some regions, the differences between the use of the word extremist(s), terrorist(s), or militant(s) may speak to the identity and/or tactics, techniques, and procedures (TTPs) of the threat actor in question. OSAC regional analysts are always ready to discuss known TTPs of various groups in a given region.
2. Timelines are a crucial piece of information in warning of a threat. If a date or date range is known, it will be included in the alert.
3. When date ranges are not known, indications of plot progression and imminence can often be inferred from the use of terms such as "observed," "surveilled," "discussed," and "planned" (often referring to aspirational or nascent planning) versus "prepared," "were ready," or "staged," which may refer to the later stages of attack plotting.

Does OSAC need anything from me?

While these alerts are rare, when they do crop up, it is vital for OSAC to be able to reach the appropriate personnel immediately. The primary recommendation for OSAC members is to keep contact information updated on OSAC.gov and to ensure that in-country staff establishes lines of communication with the RSO. OSAC staff also values feedback on the utility of the information passed, and any security measures implemented in response to the information. This feedback may inform follow-up action and/or the sharing of future notifications.

Additional questions

This product is a collection of the most commonly observed questions and points of clarification related to the sharing of DTW notifications. OSAC members who have additional questions on this topic should contact OSACThreats@state.gov.