COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
What to Do When the Government Comes Knocking

By Rebecca Rohr[1]

One of the most important roles of a compliance officer is to protect the company. There may be no better opportunity to do that than when a government representative starts asking questions—whether a law enforcement officer shows up unannounced, a government agency sends a subpoena, or regulatory staffer emails a couple questions. The stakes can be high when the government comes calling; companies can face large monetary damages and fines, exclusion from government contracting and participation in government programs, reputational and brand damage, and jail time for company employees.

It is critical that compliance professionals understand the ways that government representatives may seek information from companies, that they prepare in advance, and that they are actively involved in responding to government inquiries. Compliance officers are a key part of the response team, along with in-house lawyers and outside counsel. The compliance office is likely to be the first call when employees have questions about dealing with the government or when there is a regulatory request. Compliance officers know the company, think about risks and how to protect the company every day, and know how to help position the company to look good before regulators. This article will help compliance professionals understand the types of government requests that can arise and will help them develop a plan in advance to handle those requests. Arming themselves with this information may be one of the best ways that compliance officers can be prepared to help the company when the government comes knocking.

Search Warrants and Dawn Raids

It may be a company compliance officer's worst fear: Government agents show up unexpectedly and armed with a warrant or other immediate demand for company documents and data. The agents spend hours going through offices and file cabinets, seizing computers and devices, and requesting interviews. How the company prepares for this possibility, and how company employees conduct themselves during a search or inspection, can significantly affect the course of the investigation.

These out-of-the-blue, unannounced seizures of evidence could include an execution of a search warrant in the United States, a dawn raid in the European Union, or any type of government-authorized immediate demand for information in countries around the world. Country-specific laws that vary by jurisdiction can apply in these situations, but there are general principles to keep in mind that apply to any unannounced demand for evidence by a government authority. These principles are broken down into two categories: 1) how to prepare for a potential search and seizure and 2) what to do on the day it happens.

In the US, a judge may issue a search warrant upon a showing of probable cause, which means that there is a fair probability that evidence of a crime will be found. The Fourth Amendment requires a showing of probable cause supported by an affidavit of a law enforcement officer, and the warrant must describe the place to be searched and the items to be seized. Search warrants are issued in criminal investigations. If law enforcement officers arrive with a search warrant, it usually means that the company is being investigated for a crime or that evidence is located there and the prosecutors did not think they could obtain the evidence in a less intrusive way (such as by a grand jury subpoena, discussed below).

How to Prepare for a Search Warrant or Other Unannounced Seizure of Evidence

Compliance professionals and in-house counsel should develop written procedures to help company employees respond to dawn raids or other unexpected searches or seizures of evidence. Having government agents show up at the door with a warrant can be unsettling at best and terrifying at worst. Employees should have a list of whom to call and what to do at their fingertips. Compliance professionals can prepare a protocol based on the guidance below, with contact information for compliance and in-house lawyers. They should send it to leads at company sites, put it on a company intranet site, or otherwise make it easy for company employees to find the information —even in the heat of the moment. The protocol should be clear and easy to understand since employees surrounded by chaos and government agents will not want to wade through complicated instructions. Set up a response tree so that when one person is alerted about the raid, they know whom to contact within other functions, such as corporate communications or executive leadership.

Responding to a Search Warrant or Other Unexpected Search and Seizure of Evidence

1. Contact your legal advisor and follow their instructions.
    a. Counsel or the compliance office should be contacted immediately once law enforcement officers arrive.
    b. You may be able to request that the government officials delay their inspection until a lawyer arrives on the scene, but in some jurisdictions (like the United States), the officials can proceed despite that request.
2. Stay calm, stay professional, and stay in control of the information flow.
    a. Stay calm and help others in the office stay calm.
    b. Be polite and cooperative with the government agents at all times. Be professional and cordial. The agents will note rude and uncooperative behavior by company employees and that assuredly will not help the company's position in the investigation.
    c. If possible, designate one person as a lead to deal with the government agents so that the flow of information goes through this person.
    d. Consider sending home any nonessential employees at the site to minimize disruption.
3. Understand who you are dealing with and the scope of the inspection.
    a. Identify the lead investigator and request business cards from each member of the investigations team, or write down their names, badge numbers, and job titles.
    b. Request a copy of the warrant or document authorizing the inspection. In the US, agents are required to leave a copy of the warrant at the premises searched.
    c. Determine the scope of the inspection. Review the warrant or other document to determine the areas to be searched and the evidence to be seized. Note any limits or time periods specified. In the US, a search warrant must be authorized by a judge and will state the premises to be searched and the items to be seized; the agents have limitations on what they can gather.
4. Monitor the progress of the inspection or search.

a. Supervise the inspectors while they are on your company premises. Consider assigning a company employee to follow each member of the inspection team and keep notes on where they searched and what they reviewed or seized—and which rooms they skipped or files they ignored. These employees can take photos or videos during the search.

b. Note any questions the law enforcement officers ask or references they make to particular names of people or other companies.

c. Do not sign any consents to search without speaking with a legal advisor, especially if you are being asked to consent to a search beyond what is described in a warrant or other authorizing document.

d. Do not provide the inspectors with computer or email passwords before speaking with a legal advisor.

e. Obtain a detailed inventory of everything the agents seized during their search, and request that the inventory be signed by the lead investigator or other member of the inspection team. In the US, federal agents are required to provide this.

5. Protect privileged, confidential, and necessary information.

    a. If the agents attempt to review any attorney–client privileged materials, ask them to stop. A legal advisor later may raise a challenge to prevent the seizure of privileged materials.

    b. If the agents seize any confidential or trade-secret materials, make sure to inform them that the company views those materials as confidential or trade secrets.

    c. If the agents are seizing computers, hard drives, or other electronic devices, ask that they make forensic copies of these items rather than seizing them all to be returned later, especially if those materials are needed to conduct day-to-day business. The agents may have a forensic team available to do this.

    d. Employees should not take any action to interfere with the search. Employees should not hide or remove evidence or destroy records at any time during or after the search.

6. Contact counsel before agreeing to an interview and document as much as possible about the interviews.

    a. Before agreeing to be interviewed, or to permitting interviews, contact a lawyer. (The inspectors may be able to proceed with interviews anyway, depending on local laws). In the US, employees are not required to speak with government agents. However, the company would be wise to not prohibit employees from speaking with government agents if they want to.

    b. If the interviews are conducted by US authorities, compliance professionals should inform employees that:

        i. They are not legally required to speak with the agents, but they may choose to do so.

        ii. Anyone who does speak to an investigator should be sure to tell the truth. Lying to a law enforcement agent is a crime in the United States. Answers to questions should be short, truthful, not misleading, and accurate, without guesses or speculation.

        iii. The government can use statements made against that person or against the company.

iv. An employee has the right to counsel. Whether the company is willing to provide the counsel is a separate question, but an employee can ask that their lawyer be present.

v. The employee is free to stop the interview and leave at any time (unless the agent states differently, such as if the employee is under arrest).

c. Take notes on who was interviewed and what was asked. After the interview, ask the interviewee what questions the investigators asked and try to get as much detail as possible about the questions and answers while their memory is fresh.

7. After the agents leave, debrief and develop a communications plan.

a. When the agents leave the site, speak with employees who were present about what they observed the inspectors do or say.

b. Instruct the employees not to discuss the inspection with third parties (including customers, partners, competitors, and the press).

c. Develop a communications plan and public response.