7. Dealing with public authorities and other third parties

## 7.1. Information requests

Due to their particularly high level of potential risk and their importance for Siemens’ reputation, any impending or current criminal or administrative proceedings against Siemens or one of its employees as well as any related requests for information must be reported immediately to Compliance Investigation and Regulatory Central Function (LC CO IR CF).

Any response to such a request must be coordinated in advance with LC CO IR CF

## 7.2. Dawn raids

*(This chapter about dawn raids can be printed out or separately filed as Pdf* [*here*](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_RG_PL/findIT_LC_CO_RG_PL_7480.pdf) *in order to have the content close to hand[[1]](#footnote-1))*

In the event of an unannounced entry request by public authorities (“dawn raid”), the principles set out below must be observed to the extent permitted by local law[[2]](#footnote-2).

The principles must be adjusted in accordance with local law requirements and may be amended appropriately to provide local dawn raid guidance. Supporting documents (such as a standard notification form for security and reception staff or information on the local intranet) may be added if appropriate and in consultation with Siemens AG Legal and Compliance (Compliance Investigation and Regulatory and Legal Competition). Security and reception staff especially must be made aware of these principles and of the difference between an announced visit by the authorities and a dawn raid.

The following public authorities in particular might conduct a dawn raid:

* Public prosecutor’s office
* Investigative judge’s office and Antitrust agencies
* Police/federal/state investigative bureaus
* Tax fraud investigators
* Customs inspectors
* Secret service units
* Other public investigating agencies

|  |
| --- |
| In case of a dawn raid, please  first of all, communicate front desk to immediately inform local Compliance and Legal,  stay calm, polite and cooperate with the authority,  do not obstruct the inspection and do not conceal, alter, remove or destroy any documents or electronic data and  do not conduct informal conversations. Be factual. |

### 7.2.1. Notification

The security or reception staff where the public officials request entrance must immediately inform the assigned representative(s) of the local Legal and Compliance team (“local Legal and Compliance”). Their telephone contact details must be published appropriately, for example in the local dawn raid guidance. If available and appropriate, a central dawn raid hotline or information system can be set up to direct the information to the assigned team members.

In addition, Siemens AG Compliance Investigation and Regulatory Central Function (LC CO IR CF) must be informed immediately. In the event of an antitrust raid, Siemens AG Legal Competition (LC M&A CMP) must also be informed.

### 7.2.2. Cooperation

The public official in charge of the dawn raid (“lead official”) must be informed that it is Siemens’ general policy to cooperate with public authorities and that the notification of Legal and Compliance is intended to facilitate such cooperation.

### 7.2.3. Communication

A “communication ban” occurs when the lead official forbids all communication for a brief period of time in order to prevent the loss of evidence, in particular when conducting simultaneous searches at multiple locations. In this case, the lead official must be asked for permission to contact (1) a representative of local Legal and Compliance or, if this request is denied, (2) an external lawyer representing the company.

### 7.2.4. Identification

The lead official must be asked to identify himself/herself and his/her colleagues in order to ensure that only authorized public officials are involved in the dawn raid. The authority’s address, the name of at least the lead official and, if provided, their telephone contact details must be copied or written down and be forwarded to local Legal and Compliance.

### 7.2.5. Search warrant

The lead official must be asked to produce the search warrant. This document must then be sent by fax or e-mail to local Legal and Compliance and to [Compliance Investigation and Regulatory Central Function](https://intranet.for.siemens.com/cms/059/en/about/org/Pages/compliance_regulatory.aspx?tab=1). If the public officials do not provide a search warrant or other type of court order, they should be asked (1) which authority is conducting the investigation, and (2) what the subject of the search is, in particular, what allegations are being made.

It is important to note whether the search warrant contains restrictions as to the places to be searched, specific documents or items to be seized, limitations on the dates of the documents or the timing of the dawn raid, or other restrictions.

Local Legal and Compliance should then be consulted to clarify whether or not entry should be denied. In all cases, employees must refrain from physically obstructing the public officials.

### 7.2.6. Attendance by a lawyer

The lead official must be asked to wait until the arrival of the lawyer from or sent by local Legal and Compliance before commencing the search and seizure. Employees should not obstruct the search if the lead official declines to wait.

The public officials should be accompanied by Siemens’ security or reception staff and/or a senior employee into a meeting room to wait there together until the assigned internal or external lawyer arrives.

To the extent possible and permissible, a Siemens representative should be made available to the public officials as an exclusive contact person, preferably from senior management.

Furthermore, to the extent possible and permissible, the public officials should be accompanied throughout their search by a sufficient number of representatives from local Legal and Compliance and/or external lawyers.

### 7.2.7. Communication with affected employees on site

The affected employees on site must be informed that Siemens is in the process of cooperating with a search by an authority. Any instructions given by the lead official or by Legal and Compliance must be given immediate attention. Employees must cooperate and may not obstruct the public officials. It is forbidden to conceal, alter, remove, or destroy any documents or electronic data in the affected areas. Employees must not inform anyone not affected by the dawn raid.

### 7.2.8. IT equipment

If the dawn raid encompasses electronic data, the relevant IT department must be called in for support. Local Legal and Compliance must prepare a concept with the relevant IT department detailing how to retrieve electronic data and equipment and which stakeholders to involve.

Local Legal and Compliance must verify the exact extent of the authorities’ search and seizure powers. Some authorities may have the power to require blocking of e-mail accounts, to connect their search tools to the IT infrastructure, and to be accorded the rights of an administrator (for example under EU antitrust law). Some public officials may only have the power to seize the equipment while the review of the electronic data must be conducted by other public officials.

### 7.2.9. Communication with public officials

Any Siemens employee who is asked questions by the public officials shall indicate that he or she wishes to speak to a lawyer before answering them. This applies whether the employee is questioned as a witness or as the subject of the investigation. Local Legal and Compliance shall arrange for external lawyers to represent employees during interviews if the employee is questioned as a subject.

To the extent permissible, conversations with the public officials must be limited to organizational matters (such as the location of individual documents). Employees may be obliged to answer questions that refer to the topic of the search as set out in the search warrant (for example in the case of a search under EU antitrust law). Answers must be factual, correct and never speculative

### 7.2.10. Documentation

To the extent permitted by the public officials, copies must be made of the documents seized. In addition, all documents (whether in electronic or hardcopy form) and other items seized must be registered in an internal itemized list.

1. When public officials are inspecting or copying documents and electronic data, especially e-mails, they must be monitored and asked the following question:

Does the electronic data/document/item being searched and/or seized meet the authorized scope of the search as described in the search warrant?

If in doubt, employees must ask the public officials to allow local Legal and Compliance to check each copy or electronic file with them.

1. On conclusion of the search and seizure, the public officials must be asked for their written inventory, including a receipt, itemizing all documents and items seized (by name/description and location prior to seizure).

Moreover, the public officials shall be asked for a copy of the list of items the public officials were ordered to seize (seizure list), if available and permitted. If so provided for under local law, steps must be taken to ensure that only items on that seizure list are seized. Any items taken by the public officials but not mentioned on the seizure list might be considered to have been “surrendered voluntarily”, which could have negative implications for a subsequent legal defense. Local Legal and Compliance and Siemens AG Compliance Investigation and Regulatory Central Function must be consulted before documents are handed over to determine whether Siemens has an obligation to hand them over and whether Siemens should insist on the formal seizure of the documents or produce them voluntarily. If appropriate under applicable law, steps must be taken to ensure that all items seized are listed in the authority’s inventory as having been seized and not, for example, as having been “surrendered voluntarily”.

Prior to the voluntary submission of documents, the Siemens AG Clearing Committee must be involved via Compliance Investigation and Regulatory Central Function (for details please refer to chapter “Clearing Committee Guidance”).

### 7.2.11. Differences of opinion

If there are any differences of opinion during the search and seizure, the lead official must be asked to identify the legal basis of the action. The response must be recorded in writing.

### 7.2.12. Final report

After the public officials have left the company premises, a final report on the dawn raid must be prepared and sent to the assigned representatives of local Legal and Compliance and to Siemens AG Compliance Investigation and Regulatory Central Function. In the case of an antitrust raid, the report must also be sent to Siemens AG Legal Competition.

## 7.3. Clearing Committee

In order to assess the risks resulting from the disclosure of information and documents by Siemens to law enforcement or other governmental agencies in compliance-related matters, the “Clearing Committee” (Committee) has been established.

The Committee decides on the following matters:

* requests for disclosures of information and documents from public enforcement and similar authorities/criminal courts[[3]](#footnote-3);
* voluntary self-disclosures by Siemens.

The Committee must also be informed about mandatory self-disclosures by Siemens.

Structure and procedure

The Committee comprises

* the Chief Counsel Compliance and
* the Lead Counsel Litigation.

Once a disclosure of documents is requested or a mandatory or voluntary self-disclosure is considered, the request or consideration (case) must be submitted to the Committee.

Each case is driven by a case owner who prepares a “request for resolution” for the Committee. Such a request should contain a recommendation and an executive summary of the background to the request and should comprehensively address all relevant legal aspects and risks (see the sample e-mail at the end of this document). The request should be sent to the lawyer who is administering the Clearing Committee tracking list[[4]](#footnote-4) before submitting the request to the Committee.

For mandatory self-disclosures, the case must be submitted to the Committee for information purposes only.

* The Committee evaluates the request and the attached documents.
* The Committee takes a unanimous decision whether or not to authorize the proposed disclosure (except for mandatory self-disclosures, where the Committee is only informed).
* All relevant information is collected in a Clearing Committee case tracking list.

Further information on the legal aspects (legal privilege, advantages and disadvantages of self-disclosures) can be found [here](https://intranet.legal-compliance.siemens.com/docs/Guidance_Clearing_Committee_additional_information.doc).

A sample e-mail for the request for resolution can be found [here](https://intranet.legal-compliance.siemens.com/docs/Guidance_Clearing_Committee_Sample_email_Request.doc).

## 7.4. History of changes

|  |  |  |
| --- | --- | --- |
| **Date** | **Author** | **Major changes of binding content** |
| January 1, 2019 | Martin Petrasch, Ines Keller (Dawn Raids)  Nada Sramek (Clearing Committee) | First release through the Compliance Handbook based on Siemens Circular SC No. 226 “Global Compliance”. |
| January 1, 2020 | Koen Miezenbeek | Update due to organizational changes |

## 7.5. Contacts

Compliance Officer

The Compliance Officer responsible for your unit can be found through the following [link](https://intranet.for.siemens.com/cms/059/de/about/org/Pages/compliance_organization.aspx).

Corporate Governance Owner

The contact person for dawn raids is:

[Martin Petrasch (LC CO IR CF)](https://scd.siemens.com/luz/IdentitySearch?cn=petrasch+m&utI=I&utX=X&utT=T&rtH=H&rtS=S&rtZ=Z&rtO=O&rtAktiv=A)

[Ines Kellner (LC CO RG IR CF)](https://scd.siemens.com/luz/IdentitySearch?cn=KELLNER+INES+Z002FK3T&tcgid=Z002FK3T&c=DE&o=SIEMENS&ou=LC&l=ERL+M+WVS50&department=LC+CO+RG+CL+CHL&&utI=I&utX=X&utT=T&rtH=H&rtS=S&rtZ=Z&rtO=O&rtAktiv=A)

The contact person for the Clearing Committee is:

[Nada Sramek (LC CO IR CF)](https://scd.siemens.com/luz/IdentitySearch?cn=sramek+n&utI=I&utX=X&utT=T&rtH=H&rtS=S&rtZ=Z&rtO=O&rtAktiv=A)

1. Status of the Pdf is as of January 1st, 2020. [↑](#footnote-ref-1)
2. The measures described in this appendix must be enacted or ensured by different categories of employees. Measures 1 through 5 will generally fall within the area of responsibility of security and reception staff. Measures 6 through 13 fall within the area of responsibility of employees who are subsequently involved in the dawn raid. [↑](#footnote-ref-2)
3. The Clearing Committee process applies only to requests from public authorities with law enforcement capacity, not to requests by civil

   courts, embassies and similar. [↑](#footnote-ref-3)
4. Currently [Mrs. Nada Sramek](https://scd.siemens.com/luz/IdentitySearch?cn=sramek+n&utI=I&utX=X&utT=T&rtH=H&rtS=S&rtZ=Z&rtO=O&rtAktiv=A) [↑](#footnote-ref-4)