

MANAGING THE DISCLOSURE OF EMPLOYEE-RELATED INFORMATION

A GOOD PRACTICE GUIDE FOR EMPLOYERS

APRIL 2009

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Contents

Introduction.....	2
Why disclosures happen	4
Who will be carrying out the disclosure?	6
What may be asked?	7
Disclosure and the law	8
The employer's response	11
Summary	15

Introduction

Centre for the Protection of National Infrastructure (CPNI)

The Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides advice on protecting the country's essential services, facilities and networks from terrorism and other threats.

The national infrastructure

Nine different sectors form what is known as the national infrastructure. These provide the services which support everyday life:

- Communications
- Finance
- Health
- Emergency Services
- Food
- Transport
- Energy
- Government
- Water

CPNI provides security guidance, training and research from a physical, information and personnel security perspective. It aims specifically to reduce the vulnerabilities within these sectors, with particular emphasis on the most critical elements. Loss or disruption to any of these could cause severe economic or social consequences or even loss of life.

In addition to the nine sectors above, CPNI also provides similar advice to organisations engaged in planning and running the London 2012 Olympics.

The aim of this guidance

This document provides guidance to employers in the critical national infrastructure (CNI) on how to manage employee-related information disclosed to them by the security authorities. Employers do not currently have authoritative advice on how to deal with information disclosed to them about employees in non-National Security Vetted (NSV) posts.

This guidance does not cover instances where the employee is in a post for which NSV clearance is required. The rules which govern disclosure in these cases are different and it is likely that the employer would be contacted by their sponsor department.

This guidance will explore:

- Why and when disclosures happen
- Who will make them
- What may be disclosed
- What the person making the disclosure may ask
- Legal issues
- Next steps

While there are a number of security authorities other than CPNI that may disclose employee-related information to employers, the reason for them doing so and the legislation behind the disclosure will be different in each instance.

As such, this guidance is aimed primarily for when an employer deals with CPNI, but *may* also be useful when dealing with other officials.

What this guidance offers in all disclosure cases is advice to employers on how to manage the consequences of a disclosure of information regarding an employee. Whether the disclosure is about a member of staff working in a sensitive area who is suspected of being in contact with terrorists; or is about an employee managing the organisation's finances who is falsely claiming benefits, there are common measures which the employer can take to help manage the risk.

In writing this guidance, CPNI has consulted a range of bodies including employers from the private sector, other government departments, law enforcement agencies, as well as a range of Security Service staff, including members of CPNI and investigative and legal sections.

CPNI recommends that organisations seek professional advice, especially on employment law, when implementing or amending their personnel security measures.

This document should be read in conjunction with other guidance published by CPNI, in particular:

- [Risk Assessment for Personnel Security: a guide](#)
- [Ongoing Personnel Security: a good practice guide](#)

Why disclosures happen

On occasion, security authorities such as CPNI need to disclose employee-related information to employers. Such disclosures may take the form of:

- asking the employer for information relating to the employee or
- providing the employer with information regarding the employee

The disclosure will have resulted from intelligence gathered by the security authority which then needs to be supplemented by questions posed to the employer. Alternatively, intelligence received about an employee working in a particular post may need to be passed to the employer in order for them to make a decision regarding that person's role.

In either case it is important that the passage of information between security authority and employer, and any subsequent actions by the employer, are handled legally, proportionately and discreetly.

A failure to do so may result in complications for both the security authority and the employer, including the possibility of employment tribunals.

An example of how the consequences of a disclosure can go wrong is demonstrated below:

A company was informed by a security authority that a member of its staff, who was employed in a sensitive position, had been identified in connection with an ongoing investigation. It was not informed that the employee posed a threat to either itself or its customers, merely that the individual was in contact with persons of interest. However the security authority failed to give any advice on how best to manage the situation regarding the employee and left the employer without offering any support.

Without first exploring, by means of a risk assessment process, the consequences of continuing to employ the member of staff either in their present or an alternative role, the employer decided that the employee would be suspended with immediate effect.

Further investigation into the employee later found that, despite their contact with persons of interest, there was no indication that the employee was involved in any wrongdoing. Nevertheless, the employer was still reluctant to reinstate the employee to their previous position, but was unable to demonstrate that the employee posed a threat. As such, the employer faced an employment tribunal.

This case study illustrates many of the potential pitfalls that can occur if advice is not given to the employer on how to respond to and manage the disclosure of information to them in a proportionate way.

Investigation

There may be a number of reasons why an official from a security authority may wish to speak to an employer about one of its employees.

It is important to remember that it is highly unlikely that an official would be asking an employer for details about one of its employees if that employee represented a serious threat to the organisation. If such a threat had been identified it is likely that the police would have interceded and arrested the individual at an earlier stage. In such instances when the employer is approached by an official for information it is generally because the employee in question is of interest for some other reason.

It is not uncommon for large numbers of individuals to be identified during an investigation as having some sort of association - at times very remote - with the original subject of the enquiry. Despite potentially large numbers the security authority will need to investigate every possible lead to assess whether each individual can be eliminated from the enquiry or should be of further interest.

Therefore when an employer is contacted it may simply mean that their employee is on the periphery of an investigation and linked only tenuously to the subject of the authority's investigation. It is important not to jump to any conclusions.

On rare occasions, some kind of intelligence relating to an employee *may* be disclosed by the security authority to the employer. CPNI may recommend whether an employee should be employed or not if there was insufficient evidence for the police or security authority to have grounds for arrest.

Who will be carrying out the disclosure?

Organisations

It is possible that officials from security authorities other than CPNI may wish to speak to an employer. CPNI is more likely to be concerned with matters concerning terrorism or espionage, whereas organisations such as the Serious and Organised Crime Agency (SOCA), TRANSEC, the United Kingdom Border Agency (UKBA) or the police will have different remits.

This guidance is aimed primarily for when an employer deals with CPNI, but *may* still be useful when dealing with other officials.

It is important to remember that employee-related disclosures are rare and that when they do happen each will be different from the last, especially if a different security authority is involved. As such, an employer should be mindful of the different factors that may affect each disclosure. This may include differing legislation, for example some of the exemptions affecting disclosure in the Security Service Act will not be applicable to cases involving SOCA or UKBA. Employers should remember to treat each case independently and consult with their lawyers before any decision is made regarding the employee.

For the purpose of clarity this guidance will hereafter refer to the official carrying out the disclosure as the adviser.

Employers

It is advisable for employers to nominate an individual within their organisation to be the designated point of contact for all disclosure cases. This will usually be a senior member of the security staff although in some organisations it may be someone in another department, such as human resources.

It is recommended that employers agree and communicate details of disclosure handling procedures to appropriate teams. This will ensure that the security authority is directed to the correct person before making a disclosure.

What may be asked?

Disclosure

Prior to approaching an employer, the adviser will have consulted with colleagues to ascertain exactly why it is necessary to talk to the employer, what information can be disclosed and whether any information is required from the employer.

While each case will be unique it is likely that the adviser will be asking routine questions about an employee. These may include:

- Confirmation of identity.
- Correct spelling of a name.
- Date of birth.
- Address.
- The employee's exact role within an organisation.
- Whether there are any particular security concerns about the employee.

Such information may seem basic, but it may be enough to help complete initial enquiries. The disclosure of this kind of information does not contravene the Data Protection Act which is covered in the following chapter. However further questions about employees, such as those dealing with personal beliefs, may be constrained by various legal frameworks.

Employers will wish to consider the need to consult their legal representatives before taking any action regarding an employee following the disclosure. Further information about the legal ramifications surrounding disclosure is covered in more detail in the following chapter.

Disclosure and the law

The legislation

There are a number of legal provisions in place to help ensure that both the organisation making the request for information or disclosure and the employer responding to the disclosure are not contravening the rights of an employee.

While different organisations operate under varying remits - and some of the following legislation applies specifically to the CPNI/Security Service - different aspects will apply to other security authorities carrying out disclosures.

Individuals making a disclosure to an employer will be familiar with the relevant legislation but it is unlikely that they will be legally trained. It is therefore important that employers familiarise themselves with the legislation and, in the event of a disclosure being made, they should consult their lawyers to ensure that they are acting lawfully.

The Security Service's conduct in acquiring private information about an individual will be lawful if it is in accordance with the law, necessary for the purposes of protecting national security and proportionate to that aim.

Obligations under Article 8 of the European Convention on Human Rights

Article 8(1) of the European Convention of Human Rights (ECHR) guarantees an individual's right to respect for his private and family life, his home and his correspondence. Article 8(2) states there shall be no interference with that right by a public authority, save where that interference is in accordance with the law and necessary for one of the legitimate purposes set out in Article 9 (which include the protection of national security). The European Court of Human Rights has determined that an essential part of necessity is that the interference in question is proportionate to what it seeks to achieve. Thus interference with an individual's right to privacy must satisfy three criteria to comply with the requirements of Article 8 in that it must be:

- In accordance with the law.
- A legitimate purpose; and
- Proportionate to what it seeks to achieve.

Under Section 6 of the Human Rights Act 1998 (HRA) it is unlawful for a public authority such as the Security Service to act in a manner incompatible with a Convention right. Accordingly, where the Security Service's acquisition of information about an individual constitutes an interference with that individual's right to privacy, the Security Service conduct will be unlawful unless it meets the three criteria set out above.

In this regard, the requirement that conduct “is in accordance with the law” means that it must be authorised by, or under, domestic legislation. Furthermore, that legislation must be sufficiently precisely drafted to be foreseeable in its operation (the theory being that an individual should be able to read that legislation and determine the conduct on his part which would allow a public authority to interfere with his privacy under that legislation).

The Security Service Act

The Security Service Act 1989 (SSA) puts the Service on a statutory basis and sets out its functions. Under Section 2(2)a the Director General has a duty to ensure that arrangements are in place to ensure that the Service obtains information only to the extent that this is necessary in the proper pursuit of the Service’s statutory functions. The effect of this provision is to restrict what would otherwise be an unfettered ability to obtain information (save where to do so is otherwise lawful). From an Article 8 (of the HRA) perspective, the SSA constitutes domestic legislation authorising the Service to obtain information for the purposes of its statutory functions: the SSA is regarded as providing a basic foundation in the UK for the Service’s acquisition of information.

In certain circumstances CPNI may recommend whether an employee should be employed or not. This will only occur if the employer is one of those listed under the Provisions of the SSA¹ and the employee is not in a vetted post. Any such decision would fall under Section 2(3) of the SSA, which requires that information in the possession of the Service is only disclosed for use in determining whether a person should be employed, by any person, or any office or capacity, if they fall within these Provisions.

The Data Protection Act 1998

The Data Protection Act (DPA) provides for the regulation of processing of information about individuals, including the obtaining, holding, use and disclosure of such information. The provisions of the DPA create duties for “data controllers” and “data processors”, defining data in broad terms. They contain a series of requirements relating to the processing of “personal data”² and set out the “data protection principles” regulating the basis upon which data can be obtained, processed, retained and disclosed. The DPA also provides individuals with the right to access data about them which has been obtained and stored (subject to access rights).

Section 28 of the DPA creates an exemption from the operation of the data protection principles and certain aspects of the DPA (including its provisions in respect of subject access rights) where such an exemption is required for the purposes of safeguarding national security.

¹ The Provisions are a list of organisations, as agreed by the Secretary for State, which perform a variety of functions and hold posts that meet a number of pre-determined criteria, including long term, frequent and uncontrolled access to information or assets marked Secret or above.

² The term “personal data” is defined as meaning data relating to a living individual who can be identified from those data, or from those data and other information in the possession of, or likely to come into the possession of, the data controller.

Data processing for these purposes is also protected by a Certificate which the Home Secretary signed under section 28 of the DPA on 10 December 2001³. This certificate constitutes conclusive evidence for the purpose of the DPA that the national security exemption under section 28 is required in relation to the disclosure of data to the Service for the purposes of its statutory function.

In so far as the exemption applies, the DPA is regarded as providing a statutory basis upon which the Security Service can acquire personal data from individuals or organisations holding that data in accordance with the DPA. In other words, provided the Security Service's acquisition of the data is necessary for the purposes of safeguarding national security (which it must be for the Security Service to be able lawfully to obtain under the SSA) and proportionate to that aim, then authorisation will be deemed "in accordance with the law" for the purposes of Article 8.

Counter Terrorism Act 2008

In so far as those who provide information to the Service are concerned about breaching confidence/the confidential nature of any information provided, Section 19 of the Counter Terrorism Act 2008⁴ confirms that it is lawful for any person – whether a government department, company or individual – to disclose information to the Service for the purposes of the exercise by the Service of any of its statutory functions.

Presenting the information

When an adviser makes a request for information to an employer they will provide a letter outlining the information required and the legal justifications associated with it. It will include instructions on how to store the letter and to who it can be disseminated. The content of this letter will have been authorised by Security Service senior managers and lawyers.

If CPNI is recommending whether an employer should alter the terms of an employee's employment the adviser will present a form of words outlining relevant details about this decision. It is important to remember that CPNI will only be recommending that the employee should no longer be employed - it is a matter for the employer to decide whether to change the terms of employment. However, the adviser will be able to offer the employer some assistance on how to proceed.

³ <http://www.informationtribunal.gov.uk/Documents/nsap/gosling.pdf>

⁴ http://www.opsi.gov.uk/acts/acts2008/ukpga_20080028_en_3#pt1-pb4

The employer's response

The employer's position

Where an adviser is requesting information about an employee, an employer is not obliged to provide any information, even with the various legislative exemptions in place, and will only do so on a voluntary basis. However, if the employer is approached for information from other security authorities, it may be possible that there are different demands put upon them.

If the employer is willing to disclose the information, the adviser will not expect the requested information to be available immediately. It is understood that a director of security, for example, may not have immediate access to the shift patterns of cleaners or the job description of an engineer. It will be for the employer and the adviser to decide on how next to proceed. It may be possible for the employer to access the desired information in a matter of minutes or it may require them to consult colleagues.

What can the employer ask?

The adviser will be able to answer certain questions, however there will be limitations on what the adviser can provide. On one hand they may be constrained by what they can reveal. On the other, they may simply not know anything more than they are telling the employer. This is normal practice and should not be taken as meaning the adviser has a lack of trust in the employer.

The employer's response

It is understandable that the initial reaction of an employer, after being informed that one of their employees is of potential security interest, may be one of panic or anger and the first thought may be to confront or even dismiss the employee.

While every disclosure incident and every affected organisation is different, what is important in such cases is that the response to the disclosure is necessary and proportionate.

It is vital to remember that a disclosure about an employee does not necessarily mean that person is a threat or involved in any form of wrongdoing. It is entirely possible that the information supplied by the employer may eliminate that person from an investigation. This is important to remember, as there have been occasions when employers have made knee-jerk reactions and attempted to suspend employees about whom disclosures have been made, only to later discover there was no evidence to support this.

Nevertheless, it is understandable that an employer is going to have concerns about their employee and potential reputational risks to their organisation. The adviser will be able to provide advice on how manage this concern and possible next steps. This is covered in more detail later in this section.

Who can the information be shared with?

The security contact in the organisation may not have immediate access to the answers of the questions posed to them and may well need to speak to colleagues in other departments. While the security authority recognises that there may be a need to do this, there are potential concerns as to how many people the disclosed information is shared with.

From the security authority's point of view, there may be concerns over the sensitivity of the disclosed information and fears that if it is disseminated to too wide an audience, the subject of the disclosure may become alerted to the fact and if they are involved in any form of wrongdoing, take steps to avoid further detection. Conversely, for the employer, if too many of their employees are aware of a concern about a member of staff, the subject of the disclosure may find out and be unhappy at what they may see as unfair intrusion into their lives. The adviser will provide guidance to the employer on who the information can be shared with.

Storage of information

When the adviser presents the employer with a form of words outlining what information is requested, there will also be a paragraph on the letter's storage. It is likely the adviser will ask the employer whether they have a suitable place to store any information presented to them.

What to do next

As previously mentioned, it is understood that questions about an employee will naturally raise concerns for an employer. Generally it will be preferable, both from the point of view of the security authority and the employer, if they do not immediately dismiss the employee without any firm evidence of wrongdoing. Neither should an employee be instantaneously moved from one role to another without any prior warning; doing this may leave an employer open to a constructive dismissal charge.

In some situations, the employer may decide to carry out some form of internal investigation of an employee. Some organisations will have processes in place for doing this, whereas for others, this will be a new concept.

The employer will need to be careful to ensure that whatever action they do decide to take is necessary and proportionate. There are legal and resource implications to consider and ensuring that the investigative process is both impartial and proportionate is vital to protect the organisation's integrity and future relations with its staff.

Employers wishing to carry out an investigation need to:

- Choose the correct people for the task including a lead investigator and sponsor
- Decide whether to carry out the investigation overtly or covertly
- Clarify who else to involve, such as human resources or line managers
- Consider whether the employee should be suspended during the investigation
- Decide how to collect evidence
- Be mindful of legislation
- Consider whether to monitor the employee, mindful of internal policies.

It is important to remember that any decision made regarding an employee is the employer's responsibility. CPNI and other security authorities can only provide advice and recommendations - they cannot force an employer to make a decision.

In addition to this disclosure guidance, CPNI has produced a number of other publications⁵ that can help an employer deal with a variety of personnel security related issues (including those listed below). These publications should be considered as aids and not proscriptive documents and it is the employer's decision as to how they are used. The CPNI adviser will also be able to provide the employer with assistance, should it be needed.

Personnel Security Risk Assessment

Personnel Security Risk Assessment focuses on employees, their access to the organisation's assets, the risks they could pose to the organisation and the sufficiency of existing countermeasures. It is the foundation of the personnel security management process and is also crucial in helping security and human resources managers communicate to senior managers the risks to which the organisation is exposed. CPNI's guidance aims to help security and human resource managers:

- Conduct personnel security risk assessments in a way that balances pragmatism with rigour
- Prioritise the insider risks to an organisation
- Identify appropriate countermeasures to mitigate against those risks
- Allocate personnel security resources in a way that is cost effective and commensurate with the level of risk.

Ongoing Personnel Security

Ongoing personnel security involves protecting the organisation's assets from unauthorised use by employees, identifying and managing employees who may pose a security risk, and, where necessary, carrying out investigations to resolve suspicions or provide evidence for disciplinary procedures. *Ongoing Personnel Security* brings together advice from government departments and private organisations in a single document focusing on the key elements of an effective security culture.

Both documents are available from www.cpni.gov.uk.

⁵ www.cpni.gov.uk – Protecting your assets – Personnel Security

Employment legislation

Despite the exemptions in the legislation described in the previous chapter, employers still need to be mindful of employment legislation and any contracts staff have signed.

Furthermore, if an employer decides to conduct an investigation into an employee they should be mindful of what clauses describing possible monitoring or investigation are included in an employee's contract.

Before any steps are taken to investigate or take any other action against their employee, an employer must consult an employment lawyer for advice concerning the legal rights and responsibilities of all parties involved.

What happens next?

As each disclosure case will be different it is impossible to predict how long it will take for the information provided by the employer to exonerate, incriminate or determine whether further investigation of the employee is needed.

Whilst this will leave the employer with the potentially uncomfortable situation of continuing to employ someone there may be suspicions about, it is critical to remember that changing the terms of the employee's contract, without any evidence to support any wrongdoing, could conceivably breach an employment contract.

The adviser will do all that is possible to advise the employer on how to manage the risk, though they will not be able to disclose details of ongoing investigations.

When the investigation into the employee is complete and if that person is no longer of interest, the adviser will return to the employer with a written form of words informing them that there are no longer any grounds for concern. It is the aim of CPNI not to leave employers unclear about any concerns relating to their employees.

If the investigation reveals the need for further queries about the employee it is possible that the adviser, or one of their colleagues, may pose additional questions to the employer. This process will be repeated until a decision is made regarding the employee. Again, the adviser would provide advice and support to the employer until the process is completed.

Summary

Why disclosures happen

- On occasion security authorities, such as CPNI, may need to request or disclose information about employees to employers.
- It is important that the passage of information between the security authority and the employer - and any subsequent actions by the employer - is handled legally, proportionately and discreetly.
- An employee known to pose a significant threat is likely to have been investigated by the police or arrested. As such the employer should not jump to any conclusions when a security authority discloses information about one of its employees.
- Officials from a number of security authorities may wish to speak to an employer about their employee. This guidance is aimed primarily for when an employer deals with CPNI advisers, but *may* also be useful when dealing with other officials.

What happens during a disclosure?

- When gathering information from an employer the adviser is only allowed to request information that does not contravene the various legal frameworks surrounding the collection, disclosure and dissemination of data.
- Employers should familiarise themselves with the relevant legislation and consult their legal representatives after the disclosure process.

The response

- Employers are not obliged to provide information to a security authority. Anything they provide will be done on a voluntary basis.
- The adviser will be constrained in what additional information they can disclose to the employer.
- The adviser will request that the information disclosed to the employer is disseminated only to those colleagues that need to see it.
- Any information disclosed to an employer will need to be stored securely.
- CPNI has produced other guidance documents that will help an employer consider and manage risks following a disclosure about an employee.
- Though it is impossible to predict the timeframe in which it will happen, an indication of how an investigation into an employee is proceeding will be provided to the employer. This may include a written form of words to indicate the security authority's interest in the employee has ended.