Do you and your team recognise and challenge unusual behaviours and activity?

In response to recent terrorist events, Group Security has developed guidance on spotting and speaking out in suspicious circumstances. The guidance summarises material from Government's anti-terrorism strategy and the Centre for Protection of National infrastructure. The intention is to help colleagues identify the tell-tale signs of an insider threat, feel that they can trust their instincts and be confident to speak out. Colleagues should be able to identify unusual activity and be willing to challenge and report those behaviours which are unacceptable or unusual.

To tackle the changing threat of modern terrorism on our network we are all being asked to take greater responsibility for security – at work and in our personal lives. Our vigilance is expected when in public places (e.g. on or about the public transport network) and in our workplace. Many studies have shown that, typically, colleagues of an insider threat (i.e. someone who misuses legitimate access to commit a malicious ***act***) notice their unusual behaviour leading up to the event, but shrug it off rather than take action. This inaction has had serious consequences in many security incidents.

To maintain the security and safety of everyone, whilst we are asking people to look for unusual behaviours and activity, it will be important not to simply challenge people merely because they are different. Whilst increasing our vigilance, it is important to reflect that Network Rail is becoming more diverse and inclusive. We are employing people today who, traditionally, have not been connected with the railway e.g. more women and people from different cultures. In addition, people are increasingly feeling more comfortable about disclosing information about themselves such as about their faith or sexual orientation.

Why

As an organisation we have a duty of care to our workforce and industry colleagues as well as rail users, our neighbours and the public. Line managers need to take personal responsibility for colleague welfare, safety and security. This guidance has been developed so that line managers are able to:

- **enable the identification of a potential insider threat**
- **protect the organisation and individual workers from adverse effects**
- **identify colleagues who may require support.**

Actions

Please review the guidance below; hold conversations within your team at a team meeting or safety hour and take action as appropriate.

Guidance on spotting and speaking out in suspicious circumstances

An ***insider*** is someone who (knowingly or unknowingly) misuses legitimate access to commit a malicious ***act*** or damage their employer.

Prior to insider acts, individuals typically display a range of behaviours that are unusual and could be unauthorised or suspicious in nature. However, behaviours like these can also be displayed by people who are going through a difficult time at home or work. Either way, to protect colleagues and Network Rail, they are behaviours that need to be identified and acted upon before they escalate.

Those who work closely with individuals are likely to be best-placed to identify unusual or concerning behaviours. However, because of their close working relationships they may be reluctant to take action for fear of getting it wrong or for what might happen to their colleague. There should be no blame attached to speaking out. It is unlikely to be an insider threat and may be a welfare issue, but either way colleagues should feel able to speak up.

If you see something that you don't think is OK, say so. Look out for unusual or unexpected behaviours and actions. In all cases, confidentiality will be maintained as far as is possible to protect the individuals involved and Network Rail.

What to look out for

- Behaviours that suggest someone is vulnerable or at risk (e.g. changes in work-related attitudes/ behaviours and / or signs of struggling with critical events taking place in their private life or in the news)
- Unexpected or difficult to understand work activities that cause concern (e.g. becoming unusually secretive about work activities)
- Carrying out work related activities that are unauthorised, or may be authorised for some individuals but are not for the individual concerned.

These could look like:

- Colleagues acting differently from usual
- Colleagues doing something or accessing areas they shouldn't
- Colleagues not appearing to cope with work or their personal life
- Out of character behaviours such as working late and alone
- Meddling with another person's PC or work station
- Leaking or posting sensitive information on social media
- Colleagues radically changing their appearance
- Expressing extreme, hateful or inappropriate views of any sort, political or religious.

If it looks unusual, trust your instincts. Keep alert, and check things out if you're uncertain.

Insider activity falls into five main categories:

- Unauthorised disclosure of sensitive information, such as leaking information to the press for the purposes of reputational damage
- Process corruption, essentially altering an internal process or system for an illegitimate aim, such as fraud
- Facilitation of third party access to an organisation's assets, which could include premises, information or people
- Physical sabotage, such as starting a fire in a key operational area
- Electronic or IT sabotage, e.g. intentional damage to computer hardware.

Our environment

An inclusive environment is one in which we feel safe and secure; where we look out for each other, for our customers and our workplaces. We should each recognise our personal responsibility in making Network Rail the great place we need it to be.

Unusual and unexpected workplace behaviour by an individual we know, might suggest they are experiencing critical issues, which could be financial, work or personal related. These issues, if left ignored, could cause the individual considerable distress and also raise their vulnerability to becoming involved in insider activity. **If behaviours are identified in a timely manner, appropriate support can be put in place**. Don't be put off speaking up, doing so could result in them getting the help they need and prevent malicious activities

How to take action

If you observe a colleague behaving in an unusual and unexpected way or notice a change in their behaviour, the best thing to do is speak up, to keep everybody safe and secure. Doing so can take a number of forms:

- **Discuss:** approach the individual. "I've noticed…" "Is there anything you want to talk about?"
    - With a colleague
    - With a manager
- **If you are still concerned, report:**
    - To security via asksecurity@networkrail.co.uk (keeping line manager or HR business partner informed)
    - Or you can use our confidential speak out line 0808 143 0100 www.intouchfeedback.com/index.asp?Lid=89&Cid=4040 Or search Connect for 'Speak out'
-
- **Monitor:**
    - Watch for changes
    - Review the situation
- **Emergency:**
    - In an emergency always call 999.

In all cases, confidentiality will be maintained as far as is possible to protect the individuals involved and Network Rail.