Critical Incident Management

Version 14.0

Immigration Enforcement, Border Force, Customer Services, and Illegal Migration Intake Unit

Contents

About this guidance

This guidance sets out the Immigration Enforcement (IE), Customer Services (CS), Border Force (BF) and Illegal Migration Intake Unit (IMIU) policy for critical incident management.

The purpose of this guidance is to ensure that in the event of a critical incident occurring, there is a clear system in place for all officers to follow to ensure that the incident is managed appropriately and in a consistent manner.

Contacts

If you have any questions about the guidance and your line manager or Head of Unit cannot help you or you think that the guidance has factual errors then email IE National Command and Control Unit or Border Force National Command Centre, Customer Services Capability, Critical Incident and Business Continuity or IMIU Standards, Safety and Wellbeing.

If you notice any formatting errors in this guidance (broken links, spelling mistakes and so on) or have any comments about the layout or navigability of the guidance then you can email the Guidance Rules and Forms team.

Publication

Below is information on when this version of the guidance was published:

- version **14.0**
- published for Home Office staff on **15 July 2024**

Changes from last version of this guidance

- revised definition of what constitutes a critical incident
- removal of all aide memoire content and generic checklists
- illegal Migration Intake Unit added as a guidance subscriber
- updated contact details throughout
- wording added to reflect the role of Central Crisis Command (3C)
- revised debrief model, including 'hot' and 'cold' debriefing
- removed debrief template
- wording added to elaborate on non-conferral in the event of death or serious injury
- removed examples of critical incidents
- removed escalation process flow chart
- removed glossary of terms
- expanded definition regarding JESIP, the Joint Decision Model and the METHANE situation report

Related content
[Contents](#)

Definition of a critical incident

This section describes the standard definitions of different types of critical incidents (CI). Definitions apply to Immigration Enforcement (IE), Border Force (BF), Customer Services (CS) and Illegal Migration Intake Unit (IMIU).

In the wider context, critical incidents are incidents and events of any scale outside of the usual business activity that can result in serious consequences. They can be both operational and non-operational in nature.

An incident must meet one of these definitions to be defined as critical. There are several types of CI which depend on the scale of impact, notably if one incident goes beyond the management of one business area.

There are 3 categories of CI:

- local CI
- IE, BF, CS or IMIU national CI
- cross borders, Immigration and Citizenship (BICS) CI

Local critical incident

A local critical incident is where the outcome or consequence of that incident is likely to result in:

- serious harm to any individual
- significant community or business impact
- significant impact on the confidence of the public in IE, BF, CS or IMIU
- requiring specialist resources to support the management of the incident

Critical incidents which occur within a local business area will normally be managed locally by that business area's command and control procedure. Where a CI goes beyond the capabilities of a local command, consideration must be given to escalating the incident.

Immigration Enforcement, Border Force, Customer Service or IMIU national critical incident

A national CI is defined by one or more points in a local CI being met, and the impact of the incident and subsequent response involves more than one command within IE, BF, CS or IMIU.

A national CI is managed through a national command structure led by a National Gold Commander.

These are incidents that cause major disruption to the business, preventing the organisation from meeting its objectives and falling beyond the capabilities of business continuity management.

In the event of a national CI affecting multiple agencies or organisations, command groups may be formed through the command structures of the respective agencies.

Cross Borders, Immigration and Citizenship (BICs) national critical incident

This is where one or more of the points in a local critical incident is met and the impact of the incident and response to mitigate this impact involves more than one command within the BICS.

Related content
Contents

Critical incident stages

The life cycle of a critical incident (CI) is a standardised process and must be followed to ensure that a consistent approach is achieved which facilitates effective preparation and management of a CI to mitigate risk, as well as facilitating organisational learning in the aftermath.

The stages of a CI are defined as:

- planning for a CI
- recognising and declaring a CI
- managing a CI and preventing further escalation
- return to normality

There is no defined time limit for the life cycle of a CI. Continual risk assessment must be conducted when considering moving between the stages of this life cycle.

If issues arise at any stage of a CI, they must be either mitigated or addressed before moving to the next stage.

The National Decision Model

The National Decision Model (NDM) provides a structure for decision making. It must be used at all stages of a local CI or a national CI where Immigration Enforcement, Border Force, Customer Service or IMIU is the sole agency in control of the incident.

In the context of a CI, rationale must be recorded when making decisions which affect the planning, declaration or management of a CI, or the subsequent return to normality following a CI.

The NDM aids in structuring the rationale of any decisions which have been made. It also provides a tool to aid in the review of decisions and actions, and to facilitate organisational learning.

The National Decision Model - Graphic

Related content
Contents

Planning for a critical incident

Staff must be sufficiently trained, including working awareness of the most current and relevant policies, guidance, and legislation. Adequate resources must be made available so that the overall response to a critical incident (CI) is proportionate, effectively managed, and accountable.

Horizon scanning and risk assessment must take place at all levels to understand:

- what the present circumstances are
- what may develop
- what is the impact, or potential impact, of the incident or response
- what actions should be taken should the circumstances develop into a CI

Staff must receive development packages which are appropriate for their role and provide them with a clear understanding of their responsibilities and the underlying principles of Critical Incident Management. Emphasis should be given to decision making, record keeping and operational resilience. Responsibility for this is shared throughout the management chain – all staff must take personal responsibility to ensure they are adequately trained, and managers must maintain awareness of levels of capability and make training available where necessary.

Responsibility for production and assurance of training and development packages is held individually within Immigration Enforcement, Border Force, Customer Service and IMIU respectively, but must be derived from this guidance.

If you are developing packages derived from this guidance and are unsure of what content should be included, you can email the guidance owner, IE Critical and Post-Incident Management (IECPIM).

Related content
[Contents](#)

Recognising and declaring a critical incident

Anyone can declare a local critical incident (CI) but doing so confers responsibility. Whilst the decision to declare a critical incident should not be taken lightly, it is much better to do so, take the appropriate action and then revoke it, rather than do nothing and increase the potential for escalation.

If any of the below criteria are met, you must declare a CI:

- serious harm to any individual
- significant community or business impact
- significant impact on the confidence of the public in Immigration Enforcement (IE), Border Force (BF), Customer Service (CS) or IMIU
- requiring specialist resources to support the management of the incident

Irrespective of the above criteria, if there is indication of a failing in command or a likelihood that operational or organisational learning may be required as a result of the circumstances, declaration of a CI should be given serious consideration.

It is important that a critical incident is declared as soon as the potential for one is perceived. You do not require evidence, or for an event to have already occurred, to recognise its potential to become a critical incident.

All critical incidents that occur in BF must be reported to National Command Centre (NCC).

All critical incidents that occur in either IE or CS must be reported to National Command and Control Unit (NCCU).

All critical incidents that occur in IMIU must be reported to the IMIU Coordination Hub.

In all cases, notification must be made as soon as practicable:

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use.

Official – sensitive: end of section

The role of BF and IE / CS NCC(U) and IMIU Coordination Hub

NCC(U) and the IMIU Coordination Hub are available 24 hours a day, 7 days a week. They have access to national on call rosters, to assist with establishing a national command structure. NCC(U) and the Coordination Hub are there to provide guidance and support to the Gold, Silver, and Bronze Commanders, and to function as an information conduit to notify interested parties.

All incidents

NCC(U) and the Coordination Hub can assist in coordinating the following in the event of a critical incident:

- policy, process and coordination support and advice including access to critical incident toolkits and operational plans
- internal communications and notification ensuring accurate and up-to-date information is communicated effectively and appropriately
- consulting with the relevant teams regarding media handling and press lines
- other support and tasking from Gold and Silver Commanders

NCC(U) and the Coordination Hub are responsible for liaison with Professional Standards Unit and, outside of office hours, mandatory referrals to the Independent Office for Police Conduct (IOPC, England and Wales), Police Ombudsman of Northern Ireland (PONI, Northern Ireland) and Police Investigations and Review Commissioner (PIRC, Scotland).

Local incidents

If an incident is to be managed locally, NCC(U) or the Coordination Hub must be advised that an incident is occurring. This ensures that they can escalate the incident if necessary, and valuable time is not lost passing on information later in the event. They will be there to provide advice and specialist knowledge and can support the commanders should events escalate or continue over a long period.

Related content
[Contents](#)

Managing a critical incident and preventing further escalation

The command structure

Planning must always include contingencies regarding who will comprise the command structure should a critical incident (CI) be declared.

The command structure only comes into effect upon the declaration of a CI.

The command structure is comprised of:

- Gold – strategic
- Silver – tactical
- Bronze - operational

The command structure is role based rather than grade based, however there are suggested grades which are based on levels of authority and responsibility. Each role is allocated according to skill, expertise, location, and competency. Within this structure the Gold, Silver and Bronze Commanders have specific roles.

Gold Commander

Holds ultimate responsibility for the handling and outcome of the incident and sets the strategy for dealing with it. There will only ever be a single Gold Commander for the organisation. A suggested grade for this appointment at local level is HMI / SO / SEO and above.

The Gold Commander determines the strategy for managing an incident including any tactical parameters that the Silver or Bronze Commanders should follow. Any strategy that is dictated by the Gold Commander must be clear, concise, and open to change and adaptation based on the circumstances of the incident. The Gold Commander must retain strategic oversight of the incident. While Gold Commanders should not make tactical decisions, they will be responsible for ensuring that any tactics deployed are proportionate to the risks identified, meet the objectives of the strategy and are legally compliant.

Silver Commander

The Silver Commander is responsible for producing the tactical plan following the strategy set out by the Gold Commander. There can be more than one Silver Commander, but each must have a clearly defined and logged remit. A suggested grade for this appointment at local level is CIO / HO / HEO and above.

Bronze Commander

The Bronze Commander makes the operational decisions necessary to accomplish the Silver Commander's tactical plan. A suggested grade for this appointment at local level is IO / EO or above.

As with the Silver Commander, there can be more than one Bronze Commander, provided each has a clearly defined and logged remit. For example, an incident may require a Bronze Operational, a Bronze Communications Commander, and a Bronze Logistics Commander. These examples are not exhaustive and can be assigned in response to the scale, complexity, and demand of the incident.

The golden hour

The golden hour is the period immediately following the report of an incident, when positive action should be taken.

This may include protecting, preserving, or gathering material that may otherwise be concealed, lost, damaged, altered or destroyed. Effective action during the golden hour will increase the opportunity to support staff welfare, identify suspects, protect victims and witnesses, engage with specialist support services, and help to secure positive criminal justice outcomes.

Everyone involved in the response to an incident must help to:

- preserve life
- secure material
- minimise the amount of material that could be lost to the investigation
- maximise the chance of securing material that could be evidentially important

Every member of staff will have their own golden hour opportunities specific to their role. Irrespective of this, emphasis should always be put on mitigating the effects of the incident and any consequences of the incident becoming prolonged or escalated.

Decision logs and loggists

Accurate, complete, and detailed decision logs are crucial to the successful management of any critical incident. Every decision, however minor, must be logged ensuring that the rationale behind the decision is recorded accurately. A summary of the supporting information and any options or contingencies that were considered at the time must also be recorded. At the conclusion of any incident, these logs will be made available to the officer conducting the debrief, and if appropriate, to the investigating authorities and the courts. All logs in relation to a CI must be clear, concise, and legible.

There are practical difficulties of managing an incident whilst maintaining full and accurate notes therefore it is recommended that wherever possible, commanders appoint suitably experienced personnel to maintain the critical incident log.

The relevant commander retains ultimate responsibility for the contents of the logs and must ensure they are of a standard that would allow the commander to return to them up to 7 years later, and know why a decision was made, and defend that decision if necessary. Blank decision logs can be obtained from NCC(U) or the Coordination Hub.

Advisors

Certain critical incidents may require advise from experts, or staff members suitably trained and with in-depth knowledge in that field. At the point a CI is called, consideration should be made to contact and seek assistance from the expert in that field.

Escalating and national incidents

NCC(U) or the Coordination Hub must be informed immediately of any incident with national or serious implications for any other command. They will function as a support to any existing commanders or assist in establishing an appropriate command structure if none exists. NCC(U) or the Coordination Hub will open and maintain a critical incident log during a national incident.

If a local incident escalates beyond the control and capabilities of the local Gold Commander, NCC(U) or the Coordination Hub must be contacted immediately. They will contact the appropriate Director who will function as Gold Commander. It is their role to decide whether to declare a national critical incident. If a national critical incident is declared, NCC(U) or the Coordination Hub will notify all relevant parties.

During a national critical incident, it is likely there will be a need for IE, BF, CS or IMIU to work closely together, with direct support potentially being sought from one command by another.

Departmental Operations Centre (DOC) are a central body that work alongside NCC(U) or the Coordination Hub, offering support and guidance and acting as a single point of contact (SPOC) between the operational arena and ministers and other government departments. NCC(U) or the Coordination Hub can be directed to refer to DOC in the event of a CI escalating beyond local management.

Central Crisis Command (3C) escalation

Where possible critical incidents should be managed locally, however consideration should be made as to whether to refer to 3C for escalation or guidance if a critical incident is deemed to have met the triggers for 3C's crisis response function.

3C define triggers for crisis as:

- incidents which are overwhelming in scale, such as large scale planned events that significantly affects a department's ability to operate as normal

- cross cutting or complex incidents which require a multi-directorate response, or concurrent or escalating incidents which require joint working structures across command structures
- high-Profile incidents of such political or reputational significance that escalation is required to centrally coordinate a response

Joint Emergency Services Interoperability Programme (JESIP)

JESIP principles should be followed in the event of a CI taking place which involves agencies other than those within Immigration Enforcement (IE), Border Force (BF), Customer Service (CS) or IMIU. The aim of JESIP is to ensure that emergency responders are trained and exercised to work together as effectively as possible, at all levels of command and in response to major or complex incidents.

IE, BF, CS and IMIU are not a category responder within the Civil Contingencies Act 2004 but adhere to its principles and must have a good understanding of how emergency services work together to advise on major incident planning.

The JESIP Principles are:

- co-locate - with commanders as soon as practicably possible at a single, safe, and easily identified location near to the scene
- communicate - clearly using plain English, dropping the use of service jargon
- co-ordinate - by agreeing the lead service. Identify priorities, resources, and capabilities for an effective response, including the timing of further meetings
- jointly Understand Risk - by sharing information about the likelihood and potential impact of threats and hazards to agree potential control measures
- shared Situational Awareness – established by using M/ETHANE situational reports and the Joint Decision Model (JDM)

M/ETHANE

The M/ETHANE model is an established reporting framework which provides a common structure for sharing of information regarding a CI.

This format must be used for all incidents and be updated as the incident develops.

IE, BF, CS and IMIU do not take responsibility for declaring or managing major incidents; therefore, the ETHANE model must be used when declaring and updating the status of a CI.

Accurate situational reporting during a CI enables effective and safe management of the incident. The situational report should be updated whenever new information comes to light, or if there is a change in the information provided on the prior situational report.

M/ETHANE – Graphic

M	MAJOR INCIDENT	Has a major incident been declared? (Yes/No – If 'No', then complete ETHANE message)	*Include the date and time of any declaration.*
E	EXACT LOCATION	What is the exact location or geographical area of the incident?	*Be as precise as possible, using a system that will be understood by all responders.*
T	TYPE OF INCIDENT	What kind of incident is it?	*For example, flooding, fire, utility failure or disease outbreak.*
H	HAZARDS	What hazards or potential hazards can be identified?	*Consider the likelihood of a hazard and the potential severity of any impact.*
A	ACCESS	What are the best routes for access and egress?	*Include information on inaccessible routes and rendezvous points (RVPs). Remember that services need to be able to leave the scene as well as access it.*
N	NUMBER OF CASUALTIES	How many casualties are there, and what condition are they in?	*Use an agreed classification system such as P1; P2; P3 and dead.*
E	EMERGENCY SERVICES	Which, and how many, emergency responder assets and personnel are required or are already on-scene?	*Consider whether the assets of wider emergency responders, such as local authorities or the voluntary sector, may be required.*

M – Major incident
E – Exact location
T – Type of incident
H – Hazards
A – Access
N – Number of casualties
E – Emergency services

The Joint Decision Model

Only category responders under the Civil Contingencies Act 2004 may declare and become the lead agency on a major incident. Generally, this is an event or situation with a range of serious consequences that are beyond the scope of business-as-usual operations. Such scenarios are likely to result in serious harm, damage, disruption or risk to human life or welfare, essential services, the environment, or national security.

The Joint Decision Model (JDM) must only be used in place of the NDM when supporting a Major Incident under the JESIP principles.

Where the Home Office Code of Ethics sits at the centre of the decision-making process under the NDM, it is replaced by the JESIP principles within the JDM.

The JESIP principles around which decisions must be made when jointly working are:

- working together
- saving lives
- reducing harm

The Joint Decision Model – Graphic
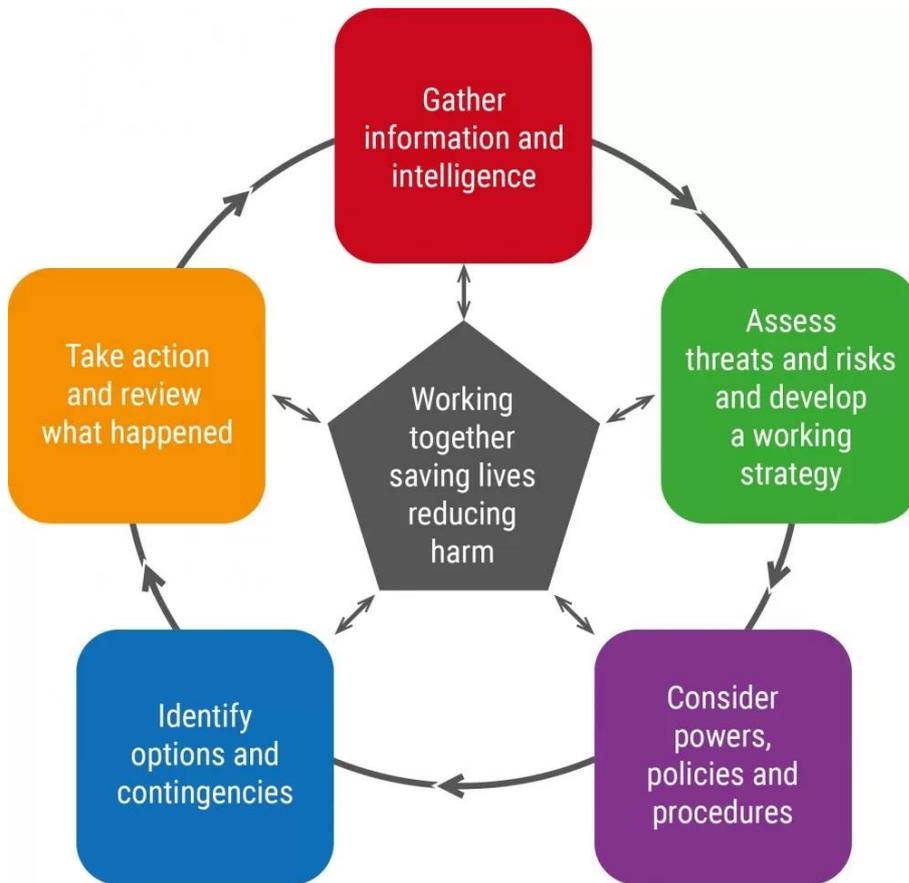
Business Continuity Management

Each business area, command or directorate has a Business Continuity Plan (BCP) in place, which will identify their most critical activities and strategic priorities and outline how to recover these activities should a disruption or multiple disruptions occur to the state of business as usual.

Copies of IE business area BCPs are centrally held by the Risk and Assurance Team in NCCU.

Copies of BF business area BCPs are held locally within NCC and BF Terminals and ports.

Copies of IMIU business area BCPs are held within IMIU Business and Development.

This guidance focuses on managing the incident itself whereas BCPs are focused on business recovery in a prioritised manner. Where appropriate, business continuity

management must run parallel and maintain close lines of communication, or officially link into the critical incident command structure.

Related content
[Contents](#)

Return to normality

Once the seriousness of an event has receded and the strategy devised by Gold Commander has been achieved, the Gold Commander must declare a formal end to the incident. This must be relayed immediately to the Silver and Bronze Commanders, and all commanders should note it in their logs. This decision must also be relayed to NCC(U) or the Coordination Hub. All paperwork relating to the incident, including extraneous notes must be collected and retained locally for 7 years.

Debrief and recovery

A debrief must be held following an incident. This must be led by the Gold Commander and involve all those who played an active part in the incident including other agencies, unless instructed otherwise. This is essential to allow the business to return to normal, to highlight any lessons learned in preventing a similar incident occurring in the future, and to air any difficulties or grievances over the handling of the incident.

Debriefing should take place in 2 stages:

- 'Hot' debriefing, which must take place as soon as practically possible following an incident and should focus on the immediate welfare and safety considerations of those involved and must also consider any ongoing organisational or operational risks, whether they are present or suspected
- 'Cold' debriefing, which should take place a minimum of 72 hours after the conclusion of the incident and should focus on organisational learning

The advice of the Employee Assistance Programme (EAP) may be sought to establish if there is a need for a psychological debrief for any of those involved, it should be remembered that participation in such a debrief is voluntary and should not take place until all the legal requirements have taken place.

A detailed written record of any debrief should be made. To ensure lessons are learned and shared, debrief notes, actions taken and recommendations arising from the debrief must be returned to NCC for Border Force (BF) incidents, the Critical and Post-Incident Management team for Immigration Enforcement (IE) incidents and the Standards, Safety and Wellbeing Team for IMIU incidents.

All debriefs must be completed on a standard template to facilitate consistent organisational learning and identification of good practice.

Debriefing templates and guidance on debriefing can be obtained from the Critical and Post-Incident Management team for IE and Customer Service, NCC for BF and IMIU Standards, Safety and Wellbeing Team.

Debrief model

As a generic guide to debriefing, the following model should be used to identify:

- any areas of good practice
- learning opportunities and recommendations from areas of good practice
- areas for improvement and development
- learning opportunities from areas for improvement and development

Debriefing following a CI must be led or commissioned by the Gold Commander.

If the incident was traumatic, the Gold Commander must arrange contact with the wellbeing team for the relevant business area, or the Employee Assistance Programme (EAP).

Investigating an incident

An investigation may take place following a critical incident. This may be conducted by local management, Professional Standards Unit (PSU) or through Independent Oversight Independent Office for Police Conduct (IOPC), Police Investigations and Review Commissioner (PIRC), and Police Ombudsman of Northern Ireland (PONI)).

PSU is the 'Appropriate Authority' for IE, BF, CS and IMIU. Referrals for investigation from IE, BF and CS are made through NCC(U), who will notify PSU in-hours and directly to the Independent Investigating Authority (IIA) for the relevant geographical area out of hours. Referrals for investigation from IMIU are made through the Coordination Hub, who follow the same process.

Referral to an IIA can result in one of the following outcomes:

- independent Investigation, in which the IIA will use their own investigators to investigate an incident or complaint
- managed Investigation, where PSU, or in some circumstances the police, undertake the investigation, with setting terms of reference and progress monitoring being conducted and controlled by the IIA
- supervised Investigation, where PSU, or in some circumstances the police, have control and direction over the investigation, with terms of reference agreed by the IIA
- local Investigation, in which PSU would conduct their own investigation with no further involvement from an IIA: although in some cases there will be a right of appeal to the IAA if the matter involves an external compliant

Referral for investigation

There is a positive duty on IE, BF, CS and IMIU to self-refer. In certain circumstances, referral to an IIA is mandatory.

All actions undertaken by IE, BF, CS and IMIU under Section 41 of the Police and Justice Act 2006 are subject to investigation by an IIA where appropriate.

Examples of criteria for mandatory referral are:

- death or serious injury
- serious assault
- serious sexual offences
- serious corruption – restricted to the specified enforcement functions in section 41 of the Police and Justice Act 2006
- criminal offences aggravated by discriminatory behaviour
- any incident which engages [Article 2 (the right to life) or Article 3 (against inhuman or degrading treatment) of the European Convention on Human Rights](#)
- attempts or conspiracies to do any of the above

These powers do not include immigration decisions, granting or refusal of asylum or giving any direction to remove persons from the United Kingdom.

If a case does not meet the mandatory referral criteria however, the circumstances are such that you suspect independent oversight is needed, discuss with NCC(U) or the Coordination Hub.

Additionally, if you are made aware of the death of a person following recent contact with IE or BF staff exercising their powers, this should also be reported to NCC(U).

If you have any doubt as to whether the circumstances surrounding a CI warrant referral for to either PSU or an IIA, you must consult with NCC(U) for IE, BF and CS, and the Coordination Hub for IMIU, who will be able to obtain guidance surrounding this.

Serious injury

A serious injury is defined as a fracture, deep cut, laceration, or any injury causing damage to an internal organ or the impairment of a bodily function.

Non-conferral guidance

There is positive obligation on officers involved in a CI to ensure all activity relating to the recording of accounts is transparent and capable of withstanding scrutiny. Where there is likely to be an investigation into an incident, either internally or externally by an independent oversight body, the following non-conferral guidance should be adhered to:

As a matter or general practice, officers and staff should not confer with others before making their accounts (whether initial or subsequent). It is important that officers and staff individually record their honest held belief of the circumstances. Therefore, there is no need for them to confer with others about what was in their mind at the time of the incident, or the events that unfolded.

This guidance should not prevent any staff member from relaying operational or safety-critical information to those involved in the ongoing management of the incident or operation. If, however, in a particular case a need to confer on other issues does arise, then, to ensure transparency and maintain confidence, where

some discussion has taken place, staff must document the fact that this has taken place, highlighting:

- time, date, and place where conferring took place
- the issues discussed
- with whom
- the reasons for such discussion

Support services

There are a variety of support services available to staff members involved in a CI both during the incident and after.

The reaction to a critical incident is a very personal experience and no one can predict what type of incident will induce a traumatic reaction. Post-traumatic stress reactions can be complex and can affect behaviour and emotional wellbeing.

The EAP is available to employees who have been involved in a critical incident. The service is also able to provide advice and support to line managers on how to deal with a particular situation. The EAP provides a 24 hour, 7 days a week support helpline.

Advice and support are also available to members through their trade union.

Trauma Risk Management (TRiM)

TRiM practitioners can offer practical support to colleagues who have dealt with a critical incident or identify when a colleague may be suffering from post-traumatic stress (PTS). This service is available to all staff whilst on duty, or those effected by traumatic events whilst travelling to and from their place of employment. Officers should speak to their nominated Gold Commander to arrange TRiM support. Self-referral can be made for TRiM support by contacting the national co-ordinator.

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use.

Official – sensitive: end of section

Mental Health First Aider (MHFA)

The Home Office has a network of staff trained in mental health first aid (MHFA). Mental health first aiders are a confidential point of contact for Home Office staff

experiencing a mental health concern or in emotional distress. They are valuable in providing early assistance to staff who may be developing a mental health concern. MHFAs are trained to spot the signs and symptoms of a range of mental health issues. They offer initial help on a first aid basis but do not offer prolonged, continuing support as they are not trained to be therapists or counsellors. MHFAs are trained to listen, reassure, and respond, even in a crisis - and even potentially stop a crisis happening. They can signpost individuals to relevant areas of support. If you require support, or would like further information, contact the dedicated inbox.

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use.

Official – sensitive: end of section

Legal advice

Home Office Legal will consider all requests to assist where an officer wishes to pursue any legal action or is the subject of legal proceedings.

Complaints

Complaints arising during or following a critical incident should be passed to the incident Gold Commander.

Any allegations or complaints received through existing complaints processes will be considered by PSU who will decide on next steps.

Formal complaints which meet the criteria for independent review should be referred as follows:

- real-time complaints whilst the incident is live – NCC(U), which should be passed to PSU as soon as practicable. IMIU complaints must be directed to IMIU Standards, Safety and Wellbeing
- complaints submitted in the weeks after an incident has closed – PSU

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use.

The information on this page has been removed as it is restricted for internal Home Office use.

Official – Sensitive: end of section

Related content
Contents

Further information and training

Further information on critical incident management and lessons learned is available from the Immigration Enforcement (IE) Critical Incident Management team.

Training and development in critical incident management is available. It is the responsibility of all directors to ensure their staff receive the relevant training. This is available from the IE Critical Incident Management team, within IE Health, Safety and Wellbeing (HSW).

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use.

Official – sensitive: end of section

Related content
[Contents](#)