



GovCertUK Guidance for WARPS

GovCertUK

GovCertUK is responsible for Computer Security Incident Response within UK Government, and provides an emergency response capability to public sector organisations that may require technical support and advice during periods of electronic attack or other network security incidents.

GovCertUK's standard office hours are: 08:30-17:00; outside of these times an on-call rota is maintained to provide a 24 hours a day, 7 days a week response capability.

Due to limited resources, GovCertUK's core constituency is Central Government. However, GovCertUK do recognise the size and importance of local government within the UK and will offer assistance where possible and appropriate.

GovCertUK can be contacted by the following methods:

Telephone:	01242 709311
Fax:	01242 709113
General Enquiries:	enquiries@govcertuk.gov.uk
Incidents & Alerts:	incidents@govcertuk.gov.uk
Restricted communications (GSI only):	govcertuk@cesg.gsi.gov.uk
Website:	www.govcertuk.gov.uk

Guidance for WARPS on Incidents Types

GovCertUK will endeavour to assist departments and agencies with incidents that are reported to them. This will hopefully assist with recovery time and reduce the impact on the reporting department. In addition, this information enables us to maintain our awareness of the types of attacks used and will also help us to monitor trends that may require the issue of an advisory to the rest of the GovCertUK constituency.

GovCertUK are particularly interested in the following incidents:

- Evidence of successful targeted attacks
- Denial of Service attacks
- Where operators are aware of attacks occurring in more than one department or agency
- Successful data exfiltration

WARPS Guidance

Guidance for WARPS on Incident Reporting

All incidents should be communicated to GovCertUK via the local WARP operator. This not only ensures that the operator has awareness of the activity, but also ensures that there is a single point of contact for GovCertUK to liaise.

Incidents should be reported to GovCertUK at 01242 709311 or incidents@govcertuk.gov.uk

Where possible as much supporting information as possible should be supplied, such as log files, internal/external IP addresses, affected Operating Systems, patch levels and policy etc.

Full procedures can be found at <http://www.govcertuk.gov.uk/reporting-an-incident.shtml>

GovCertUK Incident Categorisation and Support

GovCertUK will categorise Incidents as minor, major and critical. Incidents will be categorised on a case-by-case basis depending upon a number of factors including:

- Department or agency affected
- Impact
- Threat level
- Public Interest

The categorisation of an incident may be changed during the course of an investigation as additional information is identified or revealed.

Critical Incidents will require an immediate response. Actions by the Incident Response team may include:

- On-site response if warranted and requested
- Telephone support
- Technical analysis and advice
- The issue of an alert or briefing

Major Incidents will be dealt with in a timely fashion, usually within a working day. Action required by the Incident Response team may include:

- Telephone support
- Technical analysis and advice
- The issue of an alert or briefing
- On-site response if warranted and requested

Minor incidents may only require advice and support over the telephone, but may require more support dependant upon the organisation raising the incident. Action required by the Incident Response team may include:

- Telephone support
- The issue of an alert or briefing
- Slow-time technical analysis and support

WARPS Guidance

General

If you have any questions for GovCertUK, or if you have any questions about this report, please contact us at:

Telephone:	01242 709311
Fax:	01242 709113
General Enquiries:	enquiries@govcertuk.gov.uk
Incidents & Alerts:	incidents@govcertuk.gov.uk
Restricted communications (GSI only):	govcertuk@cesg.gsi.gov.uk
Website:	www.govcertuk.gov.uk