TOP SECRET STRAP1 COMINT

The maximum classification allowed on GCWiki is **TOP SECRET STRAP1 COMINT**. Click to report inappropriate content.

For GCWiki help contact: webteam [redacted]. Support page

Cyber Defence Operations Legal and Policy

From GCWiki

(Redirected from NDIST Legal and Policy)

Jump to: navigation, search

ArrowRight.png *See main article — **NDIST***

Cdo logo.jpg

Cyber Defence Operations is a member of MISD1, and used to be known as NDIST.

Welcome to the one-stop shop for **Cyber Defence Operations legal and policy** information!

Contents

[edit] Contacts

[redacted] is the Policy Lead for Cyber Defence Operations. She is responsible for providing legal and policy advice to the Cyber Defence Operations Team and also works with Cyber Defence Leads in IPTs. She conducts regular liaison with Mission Policy on cyber defence policy issues and is responsible for communicating updates and amendments to existing guidance, as well as the development and promulgation of new guidance. She also maintains records and awareness of staff mandatory legal and policy training.

Please contact [redacted] for questions relating to warrantry, targeting, data sharing, legalities training, analyst ideas for new ways of working etc. If she doesn't know the answer straight off, she'll find out from the relevant person in Mission Policy!

CDO's main PoC in Mission Policy-LEG is [redacted], who is the Mission Policy Lead for Cyber Defence. [redacted]provides support to CDO on new tools and analysis techniques and [redacted] deals with 2nd party data sharing.

Please note that[redacted] and [redacted] of The Products & Services Team lead on all matters relating to **reporting and release policy**. [redacted] can provide assistance in their absence. Their main PoC in Mission Policy-IPOL is [redacted], Lead for Reporting and Release Policy.

The COMPLIANCE GUIDE is an excellent source of general information on how the law applies to GCHQ's operational work.

[edit] Cyber Defence Data

[edit] Authorisations for acquiring operational data

Most of GCHQ’s operational data is acquired through its own operational activities: interception, CNE or JTRIG operations. All these forms of data acquisition are authorised either by warrants, other legal authorisations or internal approval processes.

- The majority of GCHQ’s SIGINT data is acquired under RIPA s.8(4), which authorises bulk interception of communications links where at least one end is foreign. These are sometimes known as our external warrants.
- RIPA 8(1) warrants enable ’line-access’ to a person or premises in the UK.
- ISA warrants permit CNE operations against computers. ISA Section 5 refers to computers in the UK and ISA Section 7 deals with CNE operations outside the British Islands or with UK-based CNE operations which have effect overseas.
- Network monitoring is carried out under RIPA’s Lawful Business Practice Regulations (LBPR). Such data is acquired from private networks with the consent of the host department/ organisation. Consent letters or some other form of agreement/contract are used to authorise this activity, rather than a warrant.

[edit] Other sources of data

GCHQ also has opportunities to acquire data from a variety of external collaborative sources. An internal policy authorisation called the Data Acquisition Authorisation (DAA) was introduced in November 2010. The purpose of the DAA is to authorise the acquisition by GCHQ of operational data sets from external sources, where the data is personal in nature and acquisition is not otherwise authorised by warrant or other legal or policy authorisation. Further details, including links to guidance notes and the DAA form, are on the DAA Wiki page.

[edit] Cyber Defence data classification & retention

The storage, retention and classification arrangements for CDO’s different data sources were reviewed in January 2012. The CDO data classification & retention matrix DISCOVER item 16195879 properties summarises this information.

RIPA requires GCHQ to have arrangements to minimise retention of data. GCHQ implements this safeguard through policy by specifying maximum periods of retention for categories of Sigint and IA material; the policy also caters for exceptional needs. The Compliance Guide sets out GCHQ’s data retention limits.

The following retention periods for Cyber Defence data have been agreed with Mission Policy:

Data Type	Repository	Content retention	Metadata retention	Comment
SPAY	Gordian Knot, XKS, Content Cloud	6 months	6 months – XKS definition of metadata. 2 years - RIPA definition of “communications data”	IA data selected by electronic attack signature
GORDIAN KNOT	Gordian Knot	6 months	6 months – XKS definition of metadata. 2 years - RIPA definition of “communications data”	Unselected IA data

GORDIAN KNOT	XKS, Content Cloud	30 days	30 days	Unselected IA data
SQUEAL data	XKS	30 days	30 days	SIGINT data selected by electronic attack signature
MIRAGE data	XKS	30 days	30 days	data selected by electronic attack signature
Malware material	RePortal, MWX	May be retained for as long as there is an operational reason to do so	May be retained for as long as there is an operational reason to do so	Retention subject to review every 2 years.

The case for extended retention of malware and related analysis/reporting outputs was re-affirmed by MP-LEG in February 2012. The business case and approval can be found here DISCOVER item 17226579 properties

The case for the retention of IA data (SPAY & GORDIAN KNOT)was reviewed with MP-LEG in May 2012. The business case and approval can be found here DISCOVER item 18620697 properties

[edit] GovCertUK data handling arrangements

GovCertUK occasionally take delivery of data from organisations, which are seeking GovCert help as they believe that they have been attacked electronically. OPP-LEG conducted a review of GovCert's handling arrangements to ensure that adequate protection is being given to any personal information contained within this particular category of data.

Policy on GOVCERT datahandling arrangments DISCOVER item 8472647 properties are in DISCOVER.

[edit] Cyber Defence Targeting

[edit] Targeting in Information Assurance data versus SIGINT data

Sigint and IA data feeds are obtained under different legal regimes, which impose different rules regarding the examination of data of individuals in the UK or other sensitive locations 5-Eyes. However, **GCHQ has a requirement to comply with HRA for both our Sigint and IA functions.**

- IA DATA. If you are searching a database containing purely **IA** data acquired from sensors, such as GORDIAN KNOT or SPAY, then the issue of location does not occur as this data is not obtained under a RIPA warrant but consensually under Lawful Business Practice Regulations. You will still need an HRA justification for your searches.

- SIGINT EVENTS ONLY. If you are searching a purely **Events** only database such as MUTANT BROTH, the issue of location does not occur. Therefore, you may use selectors located in the UK or 2nd Party countries without further authorisation. You will still need an HRA justification for your searches.

- SIGINT CONTENT. It is only when you are querying the **content** of communications obtained under a s.8(4) warrant, or using a database where such content is available, such as XKEYSCORE, that the issue of location becomes important for legal compliance. You will still need a valid HRA justification but you will also then need to consider what authorisation is needed for targeting sensitive locations/nationalities.

- COMBINED IA & SIGINT. When querying across **both IA and Sigint data sources**, the analyst **must** apply the SIGINT rules regarding location and nationality, regardless of where the actual data comes from.

A QUICK REFERENCE GUIDE DISCOVER item 15356368 propertiesis available to help analysts understand the authorisations required for sensitive targeting in relation to the different data sources used by CDO.

[edit] Cyber defence targeting in SIGINT (content)

The aim of Cyber defence investigations is to establish whether important national (and partner) networks have been targeted, successfully or otherwise, for information by foreign intelligence services, hacktivists or cyber criminals. SIGINT data is often used to supplement and enhance IA data.

[edit] Attacker infrastructure targeting

In order to identify entities that have been the victim of an attack or intrusion, analysts focus on the infrastructure used by the foreign adversary to conduct their malicious activity on the Internet. Infrastructure selectors are typically IP addresses, domain names and email addresses. They are the means by which an adversary delivers an attack and communicates with and controls their implants that are used to gain access to and derive intelligence from the computers of targets of interest.

Tailored guidance has been produced for CDO on the legal and policy position regarding targeting IP addresses and domains for network defence purposes in **SIGINT Content**. This includes advice on selecting material for examination relating to computers in the UK (and other sensitive locations) via GCHQ databases such as XKEYSCORE or other repositories where SIGINT content is available.POLICY FOR TARGETING COMPUTERS IN SENSITIVE LOCATIONS FOR NETWORK DEFENCE DISCOVER item 15643872 properties

An accompanying FLOWCHART DISCOVER item 14360743 properties is provided to help analysts navigate through the process.

[edit] Targeting foreign attacker infrastructure in 5-Eyes countries

Foreign CNE operators and Cyber criminals use infrastructure around the world to conduct their malicious operations on the Internet in a way that is hard to attribute. This supporting infrastructure often comprises computers located in 5-Eyes countries, that are either owned or controlled by the foreign intruder or are being used without the knowledge or consent of the legitimate owner.

The aim of targeting selectors relating to attacker infrastructure is to gain intelligence on these activities, further map their infrastructure and identify the ‘victims’ of their intelligence gathering, fraudulent or disruptive activity. This information can then be used to defend government and critical national infrastructure networks.

Guidance has been developed for CDO in relation to targeting **UK and US-based** foreign electronic attacker infrastructure in SIGINT.

POLICY FOR TARGETING UK-BASED FOREIGN ELECTRONIC ATTACKER INFRASTRUCTURE DISCOVER item 16371414 properties

POLICY FOR TARGETING US-BASED FOREIGN ELECTRONIC ATTACKER INFRASTRUCTURE DISCOVER item 14348247 properties

Please refer all targeting of UK & US selectors in SIGINT to [redacted] for approval prior to taking any action. This refers to either placing a selector on cover at a front-end dictionary via SQUEAL or using as part of a query term in a content repository e.g. XKS.

DSD, CSEC and GCSB are currently reviewing their legal/policy positions in relation to targeting attacker infrastructure based in their respective countries.

[edit] Targeting email addresses for cyber defence purposes

The underlying aim of targeting an email address differs from that of targeting an IP address or domain name that has been compromised for use in electronic attack. In the case of a compromised IP or domain that is hosted in a sensitive location, your target is the foreign actor who is cohabitating on the computer. In targeting these selectors, the aim is to obtain the traffic related to the malicious activity rather than any legitimate communications that may be present. In the case of an email address your target is the person carrying out the attack. In targeting an email, the intention is to select the communications of an individual or organisation. As such, location and nationality considerations apply when targeting via the Sigint system.

- Authorisation for the targeting of foreign selectors is achieved through GCHQ's RIPA external warrants and certificate. You do not need to seek any extra authorisation for most targeting of foreign selectors. – e.g. a Russian in Russia.
- You require a specific RIPA authorisation if you are targeting the communications of an individual in the UK. E.g. a Russian in the UK
- You must seek a policy authorisation if your targeting involves any sensitivities of location or nationality. E.g. Russian in 2nd party or UK person abroad.

Targeting rules always apply to the selector that is being targeted. See: GCHQ Compliance guide: legal authorisation flow chart

Examining events data is less intrusive than examining the content of communications. You do not need any extra authorisation to carry out a search on events data, regardless of location or nationality but you must supply an HRA justification for every search.

[edit] Combined Policy Authorisation (COPA)

The new Combined Policy Authorisation (COPA) is now live for all areas of GCHQ. For full information, please see the COPA Wiki pages. The COPA replaces Sensitive Targeting Authorisations (STA), Travel Tracking Authorisations (TTA) and authorisations to query sensitive financial data (Finint). COPA is required in similar circumstances to the old authorisations: primarily where the target is sensitive by reason of 2nd Party location or 5-Eyes nationality.

The major differences are that:

- Where the target is already on a RIPA s.16(3) authorisation, that will be taken as providing

sufficient authorisation for other activities against the same target.
- All relevant activities against the target will be recorded and, where necessary, authorised on the same form.
- COPAs will usually be authorised by nominated and trained GC8s - see List D of the “Who can sign what” list DISCOVER item 5233615 properties.

Datamining for targets in the UK has been abolished. You cannot now search in Sigint intercept repositories using a term relating to an individual located in the UK unless you have a RIPA authorisation, e.g. a s.16(3) authorisation. And if you do have one, you cannot search retrospectively, i.e. you cannot seek to retrieve material sent before the authorisation was signed. As a result, the concept of Datamining, as a distinct activity, against sensitive targets has been discontinued.

What doesn’t change is that a **full legal authorisation is still needed to target a person located in the UK**. A COPA is not sufficient.

CDO’s nominated authorisers are listed below. You may approach others on list D if the CDO authorisers are not available. (NB: [redacted]no longer needs to sign off this type of authorisation.)

CDO COPA authorisers

[redacted]

NB: Continue to run all targeting requests for US infrastructure past [redacted]. We now have a ‘generic’ STA reference to put in Halter Hitch and XKS to provide an audit trail for this targeting.

[edit] Examining UK networks for evidence of electronic attack

The aim of this activity is to establish whether significant companies and organisations based in the UK have been targeted, successfully or otherwise, for information by foreign intelligence services or cyber criminals.

In order to determine whether an entity has been the target of an attack or intrusion, analysts must focus on the ‘victim’ network to search for evidence of electronic attack. There are two aspects to this:

- Searching for known threats on UK networks

- Discovery of unknown threats on UK networks

[edit] Searching for known threats on UK networks - ANXIOUS methodology

The “ANXIOUS methodology” relates to creating an XKS fingerprint for the UK IP addresses of potential victim networks in order to tag Sigint traffic relating to these networks. This traffic may then be searched in conjunction with a signature to look for evidence of known electronic attack on these companies’ networks.

The legal and policy parameters are set out below:

- The work must meet one of GCHQ’s lawful purposes (normally National Security); you will need to ensure that companies targeted under the banner of EWB have a clear link to the national security piece as any work on EWB under ISA (and RIPA) is permitted only to the extent that national security issues are directly engaged.

- You will need to provide a justification for the entities you wish to examine, so we have this on record in case we need to justify our activity to a Commissioner. Consult with CDO Policy lead before undertaking any activity.

- The UK IP addresses must NOT be referable to an individual in UK, but rather registered to a company or organisation.

- IP addresses MUST be recorded in HALTER HITCH (or BROAD OAK) along with the reasons for their 'targeting'.

- IP addresses may form part of an XKS Fingerprint for 'tagging' data of interest in traffic already collected under GCHQ 8.4 warrants. They must not be targeted on front-end SIGINT collection systems (without further legal approval.)

- The IPs may only be queried in XKS (or DONKEY KONG) in conjunction with additional selection terms relating to the malicious activity i.e. NDIST Signatures. There should be NO discovery type activity or querying of the UK IPs alone.

- The same guidance applies if we want to target one IP address vice an IP range.

[edit] Promotion of UK IP addresses

Legal and policy position relating to the promotion of UK IP addresses of Defence sector and HMG networks DISCOVER item 13408992 properties into the Internet Buffers for the purpose of improved detection of electronic attack against these entities.

[edit] MIRANDA numbers

New MIRANDA numbers came into effect in June 2011. The most recent list can be found here: Miranda Numbers spreadsheet DISCOVER item 11840084 properties

[edit] HRA justifications

HRA justifications must clearly describe the purpose of your targeting for a non-subject matter expert. Most system auditors won't have the same level of knowledge of your activity as you do. The justifications must be understandable to someone outside CDO. This doesn't mean you have to give a lengthy description; it is about explaining in clear, concise language the reason for your activity.

Some suggestions:

- Analysis into [Chinese/intrusion set name if sensitive/ or known foreign electronic attacker] targeting of UK victim computer; legitimate user communications defeated.

- Compromised IP address used by [known Russian electronic attacker]; legitimate user communications defeated

- Malicious IP address used by unknown foreign electronic attacker; no legitimate user comms present

- Development of techniques to detect malicious network activity on mobile devices
- Investigation into covert network infrastructure (this describes the activity, but you could leave out details about whose infrastructure if this is sensitive).

[edit] Cyber Defence Tools

[edit] Development of new tools & capabilities

All systems that access, acquire or process operational data must be assessed by MP-LEG for legal and policy compliance, and have an owner who is responsible for providing assurance that the system operates in a legally complaint way.

[redacted] (MP-LEG) works with CDO's legal and policy lead to assess new CDO tools and capabilities. These include DONKEY KONG, ZooL, Palantir, Overlink, RT etc.

[edit] Events-only queries in XKEYSCORE

GTE have developed two events-only queries in XKS

- HTTP Activity Events

Use the new viewer: [redacted]

Start typing **HTTP Activity Events** in the navigation pane and the option will appear. It runs on a subset of HTTP Activity fields. The results table will not let you load up the underlying session data.

- Full Log DNI Events query

To find the Full Log Events search go to 'Search' along the top menu bar in XKS and start typing 'events' (without the quote marks) in the search bar at the top of the search form navigation menu. It will be the first option listed.

These searches will only let you query on fields that are legally classed as metadata and will not provide you with a link to the underlying sessions behind each row in the results table. This allows you to write broader queries than would otherwise be allowed, although naturally you must still ensure that all queries are justified, necessary and proportionate.

Here is the list of fields present in the results: XKS HTTP Activity Events-only query fields DISCOVER item 13069754 properties

[edit] Integration of Sigint and IA data in XKEYSCORE

XKS now allows querying across a range of data sources, which include **both IA and Sigint.**

The IA data feeds in XKS are:

- EAD-GK
- EAD-SP

Policy mitigation

1. When querying across **both IA and Sigint data sources in XKS**, the analyst **must** apply the Sigint rules regarding location in his query regardless of where the actual data comes from. This is the default position to avoid accidental error, especially with regard to selecting material for examination using IP addresses located in the UK (RIPA s.16).

2. If the analyst is **only** querying **IA** XKEYSCORES, then this issue does not arise as there are no such constraints over location and nationality.

3. However, there is the real possibility of an error when analysts are switching between IA and Sigint data. To reduce the likelihood of accidental searching on Sigint XKEYSCOREs for UK IPs without consideration of their sensitivity (perhaps by analysts more familiar with IA data), it is recommended that **whenever** using XKEYSCORE, analysts consider the sensitivity of their selector.

[edit] Exporting data from XKS

There is new guidance on the steps to take if you want to export data from XKS (e.g., sending metadata to a cloud or encrypted data to PTD services). Any user wishing to export data from the system will need to complete this form.

[edit] GATEKEEPER - Access to NSA databases

GATEKEEPER is the new NSA tool which is used to apply for, and maintain access to, many of NSA’s Databases. This means that most of the NSA databases we require access to as 2nd Parties must be obtained via GATEKEEPER. GATEKEEPER also serves to align NSA missions with those of counterpart organisations to facilitate the provision of NSA auditors for these accounts.

[redacted] is the "Access Sponsor Staff" for CDO. Please contact [redacted] with any requests for access to NSA databases. Under the new GATEKEEPER set-up there is no need to organise your own auditors.

Full details on the NSA databases this covers on the GATEKEEPER_(NSA) wiki

[edit] Communications Data requests

IRON HAND is used within GCHQ to manage the lifecycle of and to store Communications Data requests. An IRONHAND user guide is available.

A Designated Person (DP) is defined under RIPA as a person who has the authority to approve the business case for the comms data request. When using IRONHAND, only nominated GC8s and above can approve requests and they are only able to view/approve requests that have been made by their group/IPT. It is valid for a DP to create a request, but a DP cannot approve their own requests.

CDO IRONHAND authorisers

[redacted]

CDO IRONHAND requestors

[redacted] [redacted]

[redacted]

[edit] Operation-specific guidance

Op DICING legal & policy guidance - March 2011 DISCOVER item 8323306 properties

Op ARCADE CONCERT legal & policy guidance - September 2011 DISCOVER item 13464646 properties

[edit] Working with partners

[edit] Providing advice & assistance to non-HMG entities

GCHQ's functions are set out in the Intelligence Service Act 1994 (ISA).

Our "Sigint/monitoring" function is at s3(1)(a) and we are limited as to the purposes for which we can exercise that function. Work must meet one of GCHQ's lawful purposes, normally national security. Any work on EWB under ISA is permitted only to the extent that national security issues are directly engaged.

Our "IA" function is at s3(1)(b) and relates to the provision of advice and assistance about cryptography and other matters relating to the protection of information and other material. While we are not limited as to the purposes for which that function can be exercised we are limited as to who we can provide that advice and assistance to. Non-HMG recipients must be determined in order to receive such information. These determinations are limited to the provision of advice and assistance under section 3(1)(b)(ii) of ISA.

The current view from the lawyers is that it depends on the source of the information/advice. This dictates which Intelligence Services Act function GCHQ will be acting under.

- If we are providing Sigint/monitoring-derived advice (i.e. CDO is monitoring the entities' communications in some way to obtain info about a vulnerability/compromise) then we will be exercising our "Sigint/monitoring" function and can do that for whoever it is necessary to do that for but only in the interests of national security. The recipients of this advice will not need to be determined.
- If it is clearly IA advice we are providing (and not monitoring communications in order to be able to do that) then this will fall under section 3(1)(b) of ISA, and non-HMG recipients will need to be determined. This is where the determinations process comes into play.
- If the advice is a mix of SIGINT and IA advice then the current policy/LA view being developed in response to the cyber hub work is to regard this advice as falling under section 3(1)(a). The thinking behind this being that it is crucial to ensure that GCHQ doesn't lose sight of the national security imperative in its provision of "mixed" advice. Thus, following this view, "mixed" advice would fall under section 3(1)(a) and would not require determination but would need to be in the interests of national security.

It is important that staff are aware, for any particular activity, what function they are carrying out and under what legal authorisation – albeit in an increasingly joined-up Mission environment, where individuals may be in a space that overlaps across the functions. This is particularly the case for CDO, where network defence work may cut-across the two ISA functions.

- In CDO's case, our Sigint, network monitoring using sensors, CIDs work, forensics and malware analysis is all carried out under ISA s3(1)(a). In the majority of cases, CDO/GovCert output is based on blended information. That is, information about the initial threat comes from our Sigint or network monitoring capabilities and tailored advice on mitigation is added to this. This falls under the category of ISA s3(1)(a). Non-HMG recipients do not need to be determined, but information must only be shared in the interests of national security.

- In a small number of cases, CDO/GovCert outputs will be purely IA based. For example, general advice to regularly patch systems or based on information that has come from non-monitoring sources e.g. open source. This falls into the category of ISA s3(1)(b). The determinations aspect only becomes relevant when providing IA advice to non-HMG bodies. Visit these links for details of the determinations process and determined organisations

[edit] Providing Security Advice and Assistance during the Olympics

Certain organisations have been determined to receive GCHQ advice during the Olympics. This only extends to the provision of IA advice by GCHQ not the provision of information derived from monitoring. GCHQ only needs to determine the organisations if it is providing the type of advice that is catered for under section 3(1)(b) ISA, such as IA advice, not if the advice falls within its section 3(1)(a) ISA function, traditionally the SIGINT function. GCHQ cannot use the process of determination to authorise either monitoring or the provision of information derived from any monitoring (including SIGINT). The full background can be found here:Olympics - Providing Security Advice and Assistance to non-HMG bodies DISCOVER item 20205546 properties

Bodies individually determined specifically with respect to the Olympics:

- The Olympic Delivery Authority
- ATOS Origin [The London-based part of the Organisation]
- ATOS Origin Major Events [The Barcelona-based part of the organisation]
- Ticketmaster
- LOCOG

New group determination for the Games which covers: Bodies with a UK office which have been identified by the Olympics-specific Information Assurance and Cyber Security Co-ordination Group (IACSCG), Olympic Cyber Co-ordination Team (OCCT), CPNI or other Government body charged with responsibility for the security of the Olympic and Paralympic Games as being important to the safety and success of the Games between 1 May and 10 September 2012 for the provision of information security advice and assistance.

There are a number of other organisations that have been determined, the justification for which includes, but is not exclusive to, the 2012 Games. One such example is Transport for London. A full list of determined organisations can be found on the CESG website.

If you need further guidance or have an entity that does not fall under an exisiting determination, please contact [redacted]In emergencies, [redacted] are the ultimate arbiters.

[edit] Discovery of network misuse

Government network monitoring is undertaken with the express consent of system controller that such monitoring will be undertaken in the interests of national security. However, we have limited that national security purpose to being for the detection, analysis and prevention of network-based attacks against HMG computer systems (Source: Consent letter signed by host organisations). Support to DefMon would be in the interests of national security, but it does not serve the more limited purpose for which express consent was given, namely the detection etc. of network-based attack. However, advice has already been given that some activities which do not constitute network-based attack may be reported from HARUSPEX, provided that to do so is in the interests of national security. Examples of such activities include serious network misconfiguration, or the re-naming of file extensions by users in order to evade firewalls. (Source: HARUSPEX legal working aid).

The project team and legal advisers considered what would happen if in the course of the monitoring work we discovered other material that was not relevant to national security, but nevertheless indicated misuse or criminal activity through network misuse. Examples of network misuse might include illicit commercial activity or the distribution of pornography. It was agreed that we would seek legal advice on a case-by-case basis. If such activity poses no threat to national security and does not constitute serious crime, then the enabling legislation, (i.e. the Intelligence Services Act 1994 and the Security Service Act 1989), might not permit GCHQ/Security Service to obtain or disclose such information.

[edit] Second Parties

5 Eyes Policy Matrix for Sharing Cyber Security Data and Products DISCOVER item 14628328 properties

GCHQ Policy Matrix for Sharing Cyber Security Data and Products with Second Parties DISCOVER item 12961243 properties

GCHQ Policy on exchange of network defence metadata with Second Parties DISCOVER item 5262362 properties

GCHQ policy on sharing Halter Hitch eA signature database with Second Parties DISCOVER item 17718071 properties

GCHQ policy on sharing malware reporting & data with Second Parties DISCOVER item 17018793 properties

[edit] Industry partners

Over the coming months and into 2012, CDO will host a number of Industry partners as part of a project called “Use of Industry Tradecraft Uplift”. These individuals have been selected to join the team for a period of time to enhance existing tradecraft and capability.

The following principles should help staff understand the key legal and policy aspects of this type of commercial partnering in the operational workspace: Industry Tradecraft Uplift - legal & policy guidance - Sept 2011 DISCOVER item 13755932 properties

[edit] Protecting sensitive information

[edit] SIGINT source protection

Please remember that some of the Signal Related Information (SRI) in certain SIGINT data is classified as TOP SECRET STRAP 2 UKEO CHORDAL, including Case notation and Sigad in some cases.

If you are thinking of sharing data with a Second Party please take this into consideration. Your targeting may be Five Eyes sharable, but some of the other information about the source may not be (some of the data in SQUEAL XKS for example). Leave out any access related information (i.e. Case notation and Sigad)when passing data to partners. If there is a specific requirement/request for this data to be shared, speak to CDO's [redacted]. It's important to get this right to protect sources.

[edit] Commercial sensitivities

Please be mindful of commercial sensitivities when discussing successful attacks on companies. Wherever possible avoid statements about the extent and impact of such compromises and consider whether citing the company name is necessary.

Information relating to vulnerabilities and compromises of commercial entities is sensitive as it has the potential to unduly impact the company's commercial standing (e.g. share price, reputation), could give advantage to competitors or to companies seeking to win security contracts.

In addition to our own detection work on UK companies, information is often given to us confidentially and so it needs to be protected accordingly. Anything that is commercially sensitive should be protectively marked COMMERCIAL. Please apply this descriptor to relevant RT tickets and other documentation. Also be circumspect about information sharing outside CDO where there is no clear 'need-to know'.

[edit] Second Party integree access to UKEO material

MP-IPOL confirmed that it is standard practice for Second Party integrees to have access to UKEO material where the relevant business area deems it necessary and proportionate and/or where it will enable the integree to be fully integrated and do their job. The equity owner should be consulted where necessary.

[edit] Training

[edit] Operational Legalities training

GCHQ's Operational Legalities training is **mandatory** for anyone who handles or makes decisions about operational data. It must be re-taken every two years.

As of May 2011, all training is via iLearn and consists of a series of linked modules with a test at the end. There are 4 "flavours" of Certification, tailored for

- Analysis
- Capability Development
- Access & Collection

- Active Operations

To successfully complete the mandatory Operational Legalities training, you must pass the assessment, which appears in iLearn as the 5th module at the end of the Certification. And you must pass it within the required timeframe.

Almost everyone in Operations will require Operational Legalities training, as will many people in other MBUs.

See the MP-LEG e-learning Wiki pages for further details.

NEW July 2012

From 2nd July 2012, in accordance with MP-LEG instructions, ITServices will not provide new accounts on operational Sigint systems unless successful completion of the appropriate mandatory Operational Legalities training is recorded in iLearn.

This applies to accounts on all operational systems controlled by the ITServices Account Management Team, including B3M, X-KEYSCORE, LOOKING GLASS/GOLDENEYE, BLAZING SADDLES, MOONRAKER, TRITON.

[edit] USSID-18 training

In addition to GCHQ's Operational Legalities training, anyone requiring access to NSA's "raw SIGINT" tools and databases (i.e. where the data is unevaluated and unminimized) must take NSA's USSID-18 training (OVSC 1800) and pass the associated test annually.

This used to be required every 2 years but with effect from 11 June 2011 it became an annual requirement. If it's more than a year since you last took the training, you should retake it as soon as possible.

Further details on the Mission Policy e-learning Wiki page USSID-18 Training

You can check your USSID-18 record on the NSA CASPORT 2nd party web site
[redacted] Select the tab called "My Identity CUE"

[edit] USSID-18 & XKS

Everyone applying for a GCHQ XKS account, must have taken their USSID-SP0018 training. This is because a GCHQ XKS account gives you default access to Menwith Hill Station COMSAT data, which counts as a US site. This means that to get an XKS account you need to pass USSID-SP0018, even though this is just one of about 30 data sources we put in XKS. Whilst this might sound silly, we rejected the idea of making MHS an optional extra, because a) it's a good site with good data in it b) most people have USSID-SP0018 anyway and c) if you don't , then it's really quite straightforward (it's an open-book, multiple choice test) and passing it will also let you access numerous other useful tools and databases.

[edit] Legal and Policy Effects Licence (LAPEL)

From Autumn 2011, Operational Leads for Effects will require a Legal and Policy Licence before they can run Effects operations. To obtain the LAPEL, Op Leads will need to meet 2 conditions:

- Attendance at an Effects Legal and Policy training session
- Policy Skill 4 at level 2

The purpose of this “Licence” is to ensure that those responsible for running Effects operations are familiar with the legal framework in which they operate, can guide others in maintaining legal compliance and have an understanding of the specific policy and ethical issues surrounding Effects.

The LAPEL is a pre-requisite for Operations Manager accreditation.

Full details on the LAPEL wiki page