Jisc Security Operations Centre: 
Data Protection Impact Assessment 
(27/3/18)

0. Purpose of Data Protection Impact Assessment
Jisc began a project to develop a Security Operations Centre (SOC) function for the Janet network in 2016. Based on the Article 29 Working Party's Guidance published in draft in April 2017 and finalised in October 2017, this was identified as potentially requiring a Data Protection Impact Assessment under the General Data Protection Regulation (GDPR), since it involves large-scale processing of data about traffic on the network, and might be considered as using automated processing and new technological solutions.

Since the project and stakeholder consultation was already well under way it was thought better to conduct this first DPIA based on the information available in 2017 (principally the GDPR text and the Article 29 Working Party guidance) so that results could be fed back into the project, rather than wait for UK guidance by which time the service is likely to be in full operation. This also allows us to demonstrate accountability by 25th May 2018 when the GDPR comes into force. Once the UK final guidance is published, we will consider when to schedule a review to adapt this initial process to the requirements of that guidance.

1. Description of Processing Operations
Jisc's Security Operations Centre (SOC) exists to protect the security of the Janet network and its connections to customer network. The SOC consists of a group of Automated Protection Systems (APS) that aim to detect and prevent incoming attacks against the network, and a Computer Security Incident Response Team (CSIRT) that responds to incidents involving the network and its customers. Services are also offered to customers to help them protect the security of their own internal networks, systems, and data.

1.1 Legal Basis for Processing
Protecting the security of networks and information is recognised as a legitimate interest of their operators and CSIRTs by Recital 49 of the General Data Protection Regulation (GDPR). Plans and processes to detect and mitigate security breaches are considered to be one of the “appropriate technical and organisational measures” that data controllers and data processors are expected to provide under GDPR Articles 5(1)(f) and 32. According to Article 6(1)(f), processing for a legitimate interest must not be overridden by the rights and freedoms of data subjects: this “balancing test” is discussed in section 2 below.

Jisc is the data controller for personal data processed by the SOC and CSIRT functions. Where services are provided to customers that involve the customer providing additional raw data (e.g. from a local sensor) or give the customer additional access to derived personal data (e.g. alerts about individual local IP addresses), each customer organisation will be a joint data controller for the data processing involved.
1.2 How Data are Stored and Processed by the SOC

In normal operation, the Automated Protection Systems (APS) monitor the headers of packets flowing over the Janet network and aggregate these into flows between source and destination IP addresses. Where a flow, or pattern of flows, is identified as a possible threat, this traffic may be automatically re-directed to an inspection device. Here application headers and unencrypted content may be examined to determine what actions need to be taken to resolve the threat. The resulting alerts are currently reviewed by human operators to confirm whether filtering needs to be applied to the flow, to remove hostile features, before passing the filtered flow on to its intended destination. Where there is a high threat, or where this has been requested by a customer to protect a critical system, particular flows may be permanently re-directed, or filtering applied automatically prior to human review.

The CSIRT function receives reports of suspected incidents – from customers, internal systems and external reporters – performs human analysis of these reports and may recommend appropriate action to the reporter, customers, other Jisc services or external parties.

APS sensors and equipment are located in secure data centres or network points of presence and accessed remotely by staff in approved office or other locations. Where customers install internal sensors, these should be in secure locations. CSIRT servers are located in secure data centres or machine rooms; processing related to particular incident reports may be done locally in Jisc offices where appropriate. All staff must be authorised before being given access to SOC systems or data, and are given appropriate training according to their role.

1.3 Personal Data Used by the SOC

The initial stage of the APS examines the TCP/IP headers of all traffic passing its collection points. Some of the source and destination IP addresses will constitute personal data (the GDPR definition excludes, for example, the addresses of servers, proxies and address translation devices, which do not relate to a single individual); however all such data are processed in the same way, with the same safeguards, as it is not practical to identify those that are not in fact personal data. For flows that are re-directed – either because they appear to be a threat or because a customer has requested permanent re-direction of their traffic – the filtering system may process application headers and unencrypted content to the extent that this is required to remove hostile features.

Details of all flows on the network – typically comprising source and destination addresses and ports, duration, number of packets/bytes and header flags, but no content – are recorded and may be used by the CSIRT to permit historical and forensic analysis.

The CSIRT function also processes whatever personal data are included in reports they receive. This is likely to be smaller in scale than the APS data, but may cover a wider range, including unstructured data. For example, in addition to structured logfiles and alerts, this might include emails used in phishing or malware distribution; account details posted on public websites; and disk images for forensic analysis. It is possible that these may occasionally include Special Category Data: if this is discovered, the customers concerned will be alerted immediately and asked to decide whether, or to what extent, the investigation should continue.

Both APS and CSIRT functions receive threat intelligence from external sources; these may include personal data such as the IP or e-mail addresses associated with threats to the network, connected systems, or users.
1.4 Personal Data Shared by the SOC

Where the CSIRT learns of an incident or security weakness, it will normally try to contact those who need to act to remedy the problem. These communications will include the information necessary for the recipient to act, which may include personal data such as the IP address of a compromised machine, the e-mail or username of an account that appears to have suffered a security breach. In some cases it may be necessary to share relevant extracts from logfiles for the victim organisation to conduct its own investigation.

Where a security issue appears to be more widespread, Jisc tries to help other networks and organisations improve their security by providing information to trusted organisations and groups. In most cases this will not require the sharing of personal data; where this is essential for the information to be usable, measures are taken to ensure that the recipients only use that information for the purpose of improving network and information security.

Jisc may also share information – in accordance with Data Protection law – with law enforcement authorities where this is necessary for the prevention, detection or investigation of crime.

2. Necessity, Proportionality and Individual Rights

2.1 Necessity

Attacks likely to have a serious impact on the privacy and other rights of individuals are frequent and widespread on the Internet. Janet CSIRT deals with over six hundred privacy-impacting incidents each month; DDoS attacks capable of effectively disconnecting a customer organisation from the Internet occur several times a week. As recognised by the Article 29 Working Party, data controllers and network operators are expected to have processes to detect and mitigate these attacks. Furthermore, since attacks are often widespread and indiscriminate (see, for example, the Wannacry malware) these processes must cover all endpoints connected to the network. Even devices that do not themselves have privacy-affecting capabilities can cause damage to others when compromised (for example the Mirai botnet). In the sense of the GDPR – that incident detection and mitigation cannot be done effectively in any less intrusive way – the processing performed by the SOC is, indeed, necessary.

2.2 Proportionality

Even before the risk-reduction measures considered below, the nature of the SOC's processing inherently contains some safeguards.

First, all of the information processed by the first-stage Automated Protection System, and most of that processed by the filtering stage and the CSIRT, has the characteristics of pseudonyms: IP addresses and other identifiers cannot be directly linked to individuals; the linking information cannot be accessed by the SOC as it is held in the authentication, DHCP and NAT logs of individual customer organisations. Only in the case of Jisc employees – a few hundred out of the many millions of users of the Janet network – is the linking information even lawfully available to Jisc, and here there should be a formal process before such links are made.

Second, the great majority of the processing done by the SOC is automated. Humans do not need to inspect any non-malicious traffic; for most malicious traffic they will need no more than flow statistics to confirm the APS recommended filtering. More detailed human inspection, at a level that might involve personal data, should only be only needed for traffic that is unusual, but not clearly malicious. Since one of the purposes of a research and education network is to permit research into new network protocols, such traffic is likely to occur from time to time, but it is unlikely to involve
communications sent by individuals who are not aware of the research and any likely effect on privacy.

In addition to the GDPR's general requirement that any processing of personal data be proportionate, use of the Article 6(1)(f) "legitimate interests" basis requires a stronger test — that the benefits of the processing are not overridden by the rights and freedoms of the individuals. As the Article 29 Working Party note in their guidance on breach notification, the purpose of network and information security is to deliver a considerable benefit to the rights and freedoms of the individuals whose data are processed, not just to the organisations that do the processing. Since, as discussed below, the work of the Security Operations Centre is subject to strong safeguards to protect the rights and freedoms of individuals, we consider that a purpose that benefits the rights and freedoms of data subjects, combined with means of processing that minimise the risk to those rights and freedoms, ensures that the proportionality and balancing tests are clearly satisfied.

2.3 Individual Rights
The GDPR grants individuals a number of rights when their personal data are processed. Some of these (e.g. the rights of access and rectification) need to be exercised by the individual; others (e.g. the right to information and principles such as adequacy and retention) apply automatically to all processing.

The pseudonymous nature of the personal data processed by the SOC will generally mean that the access and rectification rights cannot be provided without significant privacy risk. As noted above, the SOC cannot link the IP addresses it processes with the individual users of those computers at those times. Even if a user can demonstrate that he was indeed using a particular IP address at a particular time, there is no way to ensure that he was the only person doing so. In these circumstances, access and rectification rights therefore create a significant risk of disclosing or altering personal data at the request of someone who is not, in fact, the subject of that data. GDPR Article 11 recognises that insisting on these rights would represent a strong disincentive to the use of pseudonyms, so permits data controllers to refuse requests in these circumstances.

Other rights, which do not require individuals to prove that they are the sole user of a pseudonymous identifier, are supported by the SOC.

The right to information about processing will be satisfied by the publication of this DPIA alongside Jisc’s master privacy notice. The single purpose of processing is to protect the security of networks, services, data and users: this is ensured by the dedicated function of the SOC's equipment and by contractual prohibitions on the information being used or disclosed for other purposes. Combined with the strong legal backing for network and information security, this ensures the processing has a strong legal basis and is fair. Personal data will normally only be exported from the EEA when the CSIRT reports to an external organisation that its systems or data are either vulnerable or being used in an attack. Under the Data Protection Directive, the UK Information Commissioner has allowed exporters to assess the risk of such transfers, while noting that individuals outside the EEA who are the subject of the exported information are unlikely to have the same privacy expectations. Under the GDPR we consider that such exports continue to be permitted as necessary for the legitimate interest of Jisc, its customers and users, in reducing the likelihood of being attacked from insecure external systems.

As discussed above, to be adequate to serve the purpose of network and information security, it may be necessary to process data covering all devices and networks connected to Janet; the types of data processed may vary from time to time, based on the developing threat landscape and industry
best practice on how to detect and mitigate current threats. All information processed by the SOC has a defined lifetime, after which it is deleted. Flows and other input data to the APS are automatically deleted after a pre-defined number of months; information used by the CSIRT is reviewed after incidents are closed, and only kept where, for example, it may be required for a police investigation. The right to erasure should therefore not arise, as personal data will be deleted in any case when there is no longer any legal basis to retain it. The right to object can be supported, as it does not create a privacy risk to others: however the only way that an individual can further reduce their privacy risk is to use a proxy or other device that will ensure their traffic is mixed with others using the same IP address.

The security of information is essential to the function of the SOC, since unauthorised access to its information would create many opportunities for a malicious intruder to damage network and information security. The measures taken to ensure security are described below.

3. Risks to the Rights and Freedoms of Individuals

Network and Information Security have been identified by legislators and regulators as essential protections for the rights and freedoms of individuals. However the processing that is necessary to ensure them also creates risks. The following significant risks have been identified as arising out of the activities of the SOC:

- **Illegitimate access to logfiles or flow data** could reveal the activity of particular network-connected computers. Other than for computers operated by Jisc itself, the SOC will not normally process data that can be used to link those activities to be linked to individuals (since login and address allocation records are held by individual customer or external organisations). However an attacker might be able to make that link using information from other sources, thus breaching the privacy of those individuals.

- **Illegitimate access to the content of internet traffic** is more likely to permit direct linkage to individuals. The law has typically considered unauthorised access to content as representing a greater privacy breach than access to activity data (e.g. *Investigatory Powers Act 2016*). However the SOC systems access less of this information than logfiles and flow data (only suspect traffic, not all traffic) so the impact is assessed as the same.

- Unauthorised use of the SOC’s systems to control network traffic could disrupt the flow of traffic to certain IP addresses or ranges, thus **affecting the network’s availability** to some or all users. Whether temporary unavailability creates a significant risk to any rights and freedoms will depend on the purpose for the network is being used.

The following risks were considered, but assessed as not creating significant risks to the individuals whose data are being processed:

- **Unauthorised destruction of personal data** processed by the SOC is unlikely to create a risk to those individuals’ rights and freedoms, though it would hinder any investigation or mitigation that relied on the data.

- **Unauthorised modification of personal data** processed by the SOC is unlikely to create a significant risk to rights or freedoms. The SOC’s activities are designed to protect network and information security, not to identify attackers, so any alteration should, at most, have an effect on service availability (see above) rather than directing blame to an innocent suspect.

In considering different threat sources (internal/external/environmental, accidental/deliberate) it appeared that the same risks might arise. For example the SOC’s systems could affect the network
availability as a result of deliberate action, an accidental misconfiguration, or an environmental incident such as a power cut. Those different threat sources are therefore considered in the next section, on how risks are addressed, where different measures protect against different threats.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illegitimate access to logfiles or flow data</td>
<td>High</td>
</tr>
<tr>
<td>Illegitimate access to message content</td>
<td>High</td>
</tr>
<tr>
<td>Effects on network availability</td>
<td>Medium</td>
</tr>
<tr>
<td>Unauthorised destruction of personal data</td>
<td>Low</td>
</tr>
<tr>
<td>Unauthorised modification of personal data</td>
<td>Low</td>
</tr>
</tbody>
</table>

### 4. Measures to Address those Risks

To reduce the likelihood of any event giving rise to these risks, several mitigation measures are used. These are described here, according to whether they mainly protect against internal, external or environmental threats (noting that some mitigations are effective against multiple threats), or against risks that arise out of information sharing.

#### 4.1 Internal Threat Mitigation

To reduce the risks arising out of internal threats (i.e. staff acting either carelessly or maliciously), all access to SOC systems is subject to access controls, with staff only having access to the APS functions required for their role. Managers have read access to see which IP addresses/ranges are currently subject to mitigation; Operators can enable or disable pre-defined mitigation patterns for a particular IP address or range; Analysts can both read and write data and configurations of the APS service; Administrators can control the underlying operating system and hardware.

A cyber-security portal allows designated contacts in each customer organisation to view which of their IP addresses/ranges are currently subject to mitigation (equivalent to Manager access, but limited to a single organisation). Where the organisation has subscribed to additional services, they may also be able to view alerts raised for their own internal services. This portal also allows organisational contacts to manage a whitelist of external IP addresses (for example critical cloud services) that should never be placed in mitigation. Queries from this portal to the APS system are handled via a proxy that permits only the pre-approved requests required for these functions.

Logs from the APS systems are recorded in a write-once, read-many (WORM) audit log, to prevent accidental or deliberate modification.

Operational processes – including risk management, incident management and document control – are covered by Jisc’s ISO9001 certification. All users are granted access to SOC systems as is required for their role, and are appropriately trained on how to use their access; employment contracts enforce a duty of confidentiality; security clearances are being considered for some staff. Physical access to data centres where equipment and data are stored is limited to authorised individuals.

#### 4.2 External Threat Mitigation

To reduce the risks arising out of external threats, all access to SOC systems from outside the SOC office must pass through a firewall. Connections are only accepted on specific ports from pre-defined locations; remote users must authenticate using multi-factor authentication. Remote access for contracted vendor support is additionally only enabled in agreed time-windows and is monitored throughout. All systems are patched in accordance with vendor recommendations; vulnerability scans are used to ensure that this is effective. User equipment runs appropriate endpoint protection
software and configurations; access to the internet is via a DNS resolver that implements real-time threat protection; laptops are encrypted; additional safe-browsing hardware is being evaluated.

4.3 Environmental Threat Mitigation
To reduce the risks of environmental threats having an effect on network availability, all key equipment is located in secure data centres with industry-standard protection against fire, flood and power outages. The APS equipment, apart from the inspection device itself, is mirrored across two geographically-separated data centres connected via a private optical encrypted link. Servers and workstations are backed up. In case of loss of the SOC office location, staff can access the service remotely as described above.

The most likely cause of an availability effect is therefore a loss of connectivity to, or service at, the location of the inspection device. This will only affect traffic that was selected for mitigation at that time; affected organisations would be contacted and asked whether they wanted to receive uncleaned traffic or to continue to have the suspect flows discarded.

4.4 Information Sharing Risk Mitigation
To reduce the risks arising from information sharing, the following controls are used. For incoming digital communications, encrypted channels (e-mail, VPN) are available to senders who support them. For telephone calls, CSIRT staff have access to a secure office; notes of calls may be taken on paper but are shredded as soon as they are transcribed into the incident handling system.

Encrypted channels are also used when transferring information to organisations that can support them. Information shared with threat analysis services has customer addresses either deleted or hashed, and uses of that information are limited by contract. When reporting incidents to Jisc customers, CSIRT staff use designated security contacts at each organisation. When reporting incidents externally, trusted communities with appropriate rules on information re-use (e.g. FIRST, CISP, MISP) are preferred wherever possible.

5. Conclusions
Following the risk reduction measures discussed above, the full risk assessment is as follows:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Source</th>
<th>Principal Mitigations</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illegitimate access to logfiles or flow data</td>
<td></td>
<td>Role-based access control, training, contracts, logging/audit</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Internal</td>
<td></td>
<td>Firewall, multi-factor authentication for remote access, patching/vulnerability scanning, logging/audit</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Illegitimate access to message content</td>
<td></td>
<td>Architecture (content only visible for traffic in mitigation), role-based access control, training, contracts, logging/audit</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Internal</td>
<td></td>
<td>Architecture (content only visible for traffic in mitigation), firewall, multi-factor authentication for remote access, patching/vulnerability scanning, logging/audit</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Effects on network availability</td>
<td></td>
<td>Resilient mitigation servers/locations; loss of filtering system only affects traffic in mitigation; process to restore unfiltered traffic if target site wishes.</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>External</td>
<td>As above</td>
<td>Low</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>-----</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td>Environ.</td>
<td>As above</td>
<td>Low</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Unauthorised destruction of personal data</td>
<td>Low</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised modification of personal data</td>
<td>Low</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We therefore conclude that the risks arising out of the SOC activities have been mitigated to an
acceptable level where they do not represent a high risk to the rights and freedoms of individual
users of the Janet network.

5.1 Recommended Actions
A number of additional measures were identified that should be considered to further mitigate some
risks:

- Jisc should consider whether it would be helpful to monitor the configurations of key
  systems and raise an alert when these change. At present changes made by user commands
  are logged, but monitoring the configurations themselves could provide an independent way
  to detect problems. (section 4.1)
- Jisc should continue to investigate and implement appropriate endpoint security software
  on SOC staff devices. (section 4.2)
- Jisc should confirm that appropriate security is applied to backup systems and media.
  (section 4.3)
- Jisc should document an expedited process to notify relevant customers if Special Category
  Data are identified during SOC activities, such as CSIRT investigations. (section 1.3)
- Jisc should ensure that there is a documented, controlled, process that is used when linking
  any Jisc IP or email addresses to individuals, to ensure that the conditions for pseudonymous
  processing of those identifiers are satisfied. (section 2.2)
- Jisc should remind network researchers that their traffic is more likely to trigger alerts, with
  possible impacts on both the research (if it depends on traffic being passed directly) and
  privacy (since alerts may well result in traffic being subject to human analysis). (section 2.2)
- Jisc should ensure that its documentation of the customer services provided by the SOC
  mentions the need to place any customer sensors in secure locations (1.2); reminds
  customers to take appropriate measures to prevent misuse of data (4.1); and notifies them
  of the process that will be followed if there is an outage at the filtering service (4.3).

5.2 Recommended Next Steps
The operation of the SOC against its documented policies is subject to both internal and external
audits under Jisc’s ISO9001 and (for some activities) ISO27001 certifications.

The Article 29 Working Party has suggested that a DPIA process should be repeated every 3-5 years.
Since this DPIA was conducted before final UK guidance was available, it should be repeated sooner,
perhaps in 12-18 months’ time. This will also allow a more detailed consultation with users, based on
this DPIA report, as part of that process.

This DPIA report should be published.

Approved (Data Protection Officer)  [Signature]  Date 10/5/2018
Approved (Senior Responsible Owner) [Signature]  Date 10/5/18
Approved (SIRO) [Signature]  Date 14 May 18