IMPLEMENTING SIPS GUIDANCE WITH ILLUMIO

Financial institutions are an attractive target for malicious actors. Incidents affecting their Systemically Important Payment Systems (SIPS) not only can result in substantial financial losses, but also have the potential to cause huge damage to the global economy, and the safety of consumers – no less than any other sector of critical infrastructure.

Breaches like the 2016 Bangladesh Bank Heist prompted new regulations addressing the security of SWIFT payment messaging systems, while regulations governing the Payment Card Industry (PCI) prescribe protections for credit card processing.

With the advent of Revised Payment Service Directive (PSD2), payment systems will be more interconnected than ever, and institutions need to protect the data processed by those systems as well.

GUIDANCE FOR FINANCIAL MARKET INFRASTRUCTURES

In June 2016, the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) published their Guidance on cyber resilience for financial market infrastructures (FMIs), which requires FMIs to immediately take the necessary steps to implement specific protections for critical systems, to ensure that they enhance their levels of cyber resilience.

Like SWIFT and PCI, one goal of these measures is to increase cyber resilience and prevent the spread of breaches to high-value financial systems. This is accomplished by deploying additional protections to isolate these assets from the rest of the network through a security enforcement measure called segmentation.

HOW CAN ILLUMIO HELP?

The Illumio Adaptive Security Platform® (ASP) uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data centre, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. Illumio ASP can help SIPS operators reduce cyber risk and achieve the outcomes specified by the SIPS Guidance principles outlined below.

2.2 IDENTIFICATION

This chapter of the Guidance outlines areas where an FMI should identify and classify business processes and information assets as well as external dependencies.

EXPECTATIONS – "EVOLVING"	HOW ILLUMIO CAN HELP
The FMI should identify and document all processes that are dependent on third-party service providers and identify its interconnections, and update this information on a regular basis.	Illumio's real-time application dependency map provides visibility into traffic flow summaries, allowing application owners to understand the data link status; policy is defined to govern them. With the application dependency map, organisations are able to: ▪ Eliminate blind spots inside and across data centre and cloud environments with a comprehensive view of application traffic. ▪ Gain granular visibility into workload relationships with details down to the flow and service level. ▪ Visualise connections to external APIs, such as those used in PSD2 and OpenBanking initiatives. ▪ Understand application dependencies on common services (e.g., Active Directory, Exchange, database platforms). ▪ See the vulnerable paths that a bad actor can exploit across environments, including connections to SaaS platforms, and external API-driven technologies. ▪ Create optimal micro-segmentation policies in minutes with automated policy recommendations. ▪ Model security policy and receive visual feedback in real time to eliminate risk of breaking applications with new policies. ▪ Pinpoint unauthorised communications and stop them immediately with the ability to quickly quarantine workloads.
The FMI should maintain an up-to-date inventory of all the critical functions, key roles, processes, information assets, third-party service providers and interconnections. It should integrate identification efforts with other relevant processes, such as acquisition and change management, in order to facilitate a regular review of its inventory.	Illumio's real-time application dependency map allows for detailed network diagrams and dependencies to be mapped and updated as changes occur – with potential alerts on changes to network traffic as they happen. Connections to new/unknown workloads can be flagged and alerted against, with context data to give responders a way to analyse the situation quickly, in conjunction with technologies such as SIEM. Integrations with change management/CMDB platforms allows bilateral communication and modification as required.
The FMI should create and maintain a simplified network map of network resources with an associated plan addressing IPs which locate routing and security devices and servers supporting the FMI's critical functions, and which identify links with the outside world.	Illumio ASP is specifically designed to monitor internal East-West traffic, which comprises around 80 percent of data centre traffic flow. As a host-based technology, granular information is available from monitored workloads, and segmentation strategies down to port/protocol/process can be applied dynamically. Using application-centric dependency mapping, Illumio groups workloads based on attributes or metadata rather than physical location, IP address, or other infrastructure constructs. The application dependency map also shows specific connections the outside world or defined network segments.

EXPECTATIONS – "ADVANCING"	HOW ILLUMIO CAN HELP
The FMI should also maintain up-to-date and complete maps of network resources, interconnections and dependencies, and data flows with other information assets, including the connections to business partners, internet-facing services, cloud services and any other third-party systems. It should use these maps to undertake risk assessments of key dependencies and apply appropriate risk controls, when necessary.	In addition to the "Evolving" expectations, the platform can support the "Advanced" requirements by mapping upstream and downstream dependencies to cloud services, external business units, third-party systems, and DNS-based serverless platforms, such as Lambda services. These can include connections via APIs to other financial services, such as those used in the Payment Services Directive 2 (PSD2) or Open Banking.

EXPECTATIONS – "INNOVATING"	HOW ILLUMIO CAN HELP
The FMI should identify the cyber risks that it bears from or poses to entities in its ecosystem and coordinate with relevant entities, as appropriate. This may involve identifying common vulnerabilities and threats, and taking appropriate measures collectively to address such risks, with the objective of improving the ecosystem's overall resilience.	Using a combination of application dependency mapping and vulnerability data, identification of the most "exposed" workloads is easily visible. Vulnerability exposure scores are calculated as a combination of network connectivity and network-leveraged vulnerability information, including "inherited" risk from upstream applications and other areas of the ecosystem.

2.3 PROTECTION

This chapter provides guidance on how FMIs should implement appropriate and effective measures in line with leading cyber resilience and cybersecurity practices to prevent, limit or contain the impact of a potential cyber event.

PROTECTION OF PROCESSES AND ASSETS

Control Implementation and Design

EXPECTATIONS – "EVOLVING"	HOW ILLUMIO CAN HELP
The FMI should implement a comprehensive and appropriate set of security controls that will allow it to achieve the security objectives needed to meet its business requirements. The FMI should implement these controls based on the identification of its critical functions, key roles, processes, information assets, third-party service providers and interconnections, as per the risk assessment in the identification phase. The security objectives may include ensuring: *(a) the continuity and availability of its information systems;* *(b) the integrity of the information stored in its information systems, while both in use and transit;* *(c) the protection, integrity, confidentiality and availability of data while at rest, in use and in transit;* *(d) conformity to applicable laws, regulation and standards.*	Illumio ASP is a security segmentation platform providing adaptive security controls for the critical applications and environments in use today. Illumio ASP is specifically designed to monitor internal East-West traffic, which comprises around 80 percent of data centre traffic flow. As a host-based technology, granular information is available from monitored workloads, and segmentation strategies down to port/protocol/process can be applied dynamically. Critical applications, environments, and workloads can be closely monitored for new, out-of-policy connectivity and output to other systems for analysis; or quarantined directly using Illumio's micro-segmentation functionality. Feeding new connection information from Illumio ASP to correlation technologies such as a SIEM allows comparison to threat intelligence information, vulnerability data, and attack vector simulation. A compromised workload will appear immediately in Illumio's application dependency map view with new attempted network connections clearly highlighted. In addition, process information tied to these network connections is also fed back into the system and upstream components for further investigation. Lastly, using Illumio's SecureConnect feature, the incumbent host-based firewalls within the relevant workloads can be configured to set up IPsec in transport mode – encrypting all or selected data links as they traverse untrusted environments.

EXPECTATIONS – "INNOVATING"	HOW ILLUMIO CAN HELP
The FMI should apply a defence-in-depth strategy in line with a risk-based approach, i.e. it should implement multiple independent security controls so that if one control fails or a vulnerability is exploited, alternative controls will be able to protect targeted assets and/or processes.	As a security segmentation overlay technology, Zero Trust networking at its core, Illumio ASP provides granular segmentation controls and the native ability to monitor workload condition for tampering. If a workload is compromised, other workloads within the environment can automatically block connectivity to the compromised OS in stance or container. Customers often maintain perimeter firewalling controls with our application-based segmentation technology providing East-West segmentation policy.

Network and Infrastructure Management

EXPECTATIONS – "EVOLVING"	HOW ILLUMIO CAN HELP
The FMI should seek to use a separate and dedicated network for information system administration. At a minimum, the FMI should prohibit direct internet access from devices or servers used for information system administration whenever possible.	Illumio ASP is designed to apply the exact level of enforcement needed for any environment, application, and workload by providing a range of segmentation options enforced at each protected workload. With Illumio, you can separate large environments like production and development with a single rule, micro-segment a specific high-value application, define granular policy for control down to the process level, and even encrypt traffic between workloads and environments with a single policy. User administration is full role-based access control (RBAC), allowing separation of duties around policy creation and sign-off, and view/control over only the relevant areas of the environment depending on jurisdiction. Access to specific administrative network segments or the internet are easily identified on the application dependency map can be alerted against by way of output to SIEM technologies.
The FMI should deploy a broad range of technologies and tools to detect and block actual and attempted attacks or intrusions. The FMI may use intrusion detection or prevention systems, end point security solutions (e.g. antivirus, a firewall, or a host intrusion detection system (HIDS) or host intrusion prevention system (HIPS)) or any other relevant solutions (e.g. an access gateway or a jump box), in particular on devices and in environments used for accessing the FMI network remotely.	Illumio ASP allows application-centric orchestration of existing enforcement points on the network to apply broad or granular security segmentation policy across any type of infrastructure at scale. Existing host-based firewalls, network switches, load balancers and, shortly, network security groups can all be centrally managed and controlled to provide environmental separation, ringfencing of high-value applications, whether on-premise or in the cloud, prevention of lateral movement and reduction of attack surface on hardware servers, VMs, containers, and even against serverless offerings such as Lambda services.
The FMI should implement controls that manage or prevent non-controlled devices to connect to its internal network from inside or outside the premises to ensure that activities in these zones are logged and monitored for inappropriate use or attempts to access business systems. The FMI's infrastructure should be scanned regularly to detect rogue devices and access points.	Using a platform feature called Machine Authentication, PKI infrastructure can be leveraged to make sure only controlled devices are allowed access to critical applications and environments. Outside of Machine Auth, the Zero Trust networking model employed by Illumio ASP means that new traffic flows, or flows to/from new workloads, are automatically blocked. Notification on traffic to and from new devices can be flagged via output to relevant alerting mechanisms such as a SIEM tool.
The FMI should scan its legacy technologies regularly to identify potential vulnerabilities and seek upgrade opportunities. Controls and additional defence layers should be implemented and tested in order to protect unsupported or vulnerable systems.	Illumio ASP can take in vulnerability data and map it to network port exposure, defining micro-segmentation policies in response to prevent exploitation of vulnerabilities before patches can be applied. Used as a compensating control, machines that are difficult to patch can be protected, and vulnerabilities that are yet to be patched at all can be prevented from being exploited by threat actors.
The FMI should implement a defence-in-depth security architecture, based on the network and data flow diagrams that identify hardware, software and network components, internal and external connections, and type of information exchanged between systems. As required in the identification phase, the FMI should maintain current and complete network and data flow diagrams.	Policy creation within Illumio ASP is built from the application dependency mapping itself – allowing segmentation policy to be created reflecting observed traffic itself. This allows for quick and accurate Zero Trust policies to be created, allowing only application traffic as needed and automatically preventing extraneous communication.
The FMI should segment its network infrastructure with security policies appropriate to its use and commensurate to its risk score, which define proper access policy to systems and applications. Sensitive traffic between systems and zones should be segregated using network management.	Segmentation is at the core of the Illumio platform – and is the primary function that Illumio ASP was built to accomplish. Utilising existing enforcement points to control traffic, in conjunction with an application-centric dependency map, allows for rapid segmentation policy to be written. The multiple modes within the platform allow for testing of policy against known traffic, with simple visual indication of allowed or denied traffic. Users of Illumio ASP typically start securing the most at-risk or valuable applications and environments first and observing flows into and out of neighboring areas before extending the platform.
The FMI's IT environments and functions should be adequately separated with different security levels and controls implemented.	See above.
The FMI should consider implementing technical measures (e.g. network access control (NAC) solutions) in order to prevent unauthorised devices from being connecting successfully.	Using a platform feature called Machine Authentication, PKI infrastructure can be leveraged to make sure only controlled devices are allowed access to critical applications and environments. Outside of Machine Auth, the Zero Trust networking model employed by Illumio ASP means that new traffic flows or flows to/from new workloads are automatically blocked. Notification on traffic to and from new devices can be flagged via output to relevant alerting mechanisms such as a SIEM tool.

Logical and Physical Security Management

EXPECTATIONS – "EVOLVING"	HOW ILLUMIO CAN HELP
The FMI should develop appropriate controls (e.g. encryption, authentication and access control) to protect data at rest, in use and in transit. The controls should be commensurate to the criticality and the sensitivity of the data held, used or being transmitted, as per the risk assessment conducted in the identification phase.	Using Illumio's SecureConnect feature, the incumbent host-based firewalls within the relevant workloads can be configured to set up IPsec in transport mode – encrypting all or selected data links as they traverse untrusted environments. Machine Authentication provides PKI-based authentication of hosts on the network, preventing any non-trusted machines from successfully communicating with critical applications or environments.

Supplier and Third-Party Security Management

EXPECTATIONS – "EVOLVING"	HOW ILLUMIO CAN HELP
The FMI should maintain and regularly update an inventory of its participants and third-party service providers, and ensure that its cyber resilience framework addresses its interconnections with the aforementioned entities from a cyber risk perspective.	Illumio ASP shows flows into network segments that do not have to be covered explicitly by the platform itself, allowing output and updating of configuration management systems such as CMDBs – becoming a more accurate source of truth while also allowing policy to be created and adapted automatically.

EXPECTATIONS – "ADVANCING"	HOW ILLUMIO CAN HELP
The FMI should design security controls that detect and prevent intrusions from third-party connections.	The default-deny policy model within Illumio ASP means that new attempted network connections are denied implicitly when the platform is running in the "enforced" mode. Any new flows can be sent out by means of feeds or taken as event data, allowing relevant systems to alert against attempts at lateral movement or compromise on the network. Built-in functionality around anti-tampering and auto-quarantining prevents compromise of Illumio ASP components on hosts themselves, and isolates systems if they are seen to be behaving in a malicious fashion.
The FMI should ensure that there are appropriate procedures in place to isolate or block its third-party connections (in a timely manner) if there is a cyber attack and/or a risk of contagion.	With a combination of network visualisation/alerting on new connections, with data analytics platforms such as a SIEM alerting against new/unusual behavior, a change of policy to further restrict network access or quarantine a workload can be realised automatically. The default-deny/Zero Trust network model used in Illumio ASP means that attack surface is naturally reduced to prevent the spread of malicious code or the actions of a bad actor.

2.4 DETECTION

This chapter of the Guidance outlines monitoring and process-related guidance aimed at helping FMIs detect cyber incidents.

EXPECTATIONS – "EVOLVING"	HOW ILLUMIO CAN HELP
The FMI should have capabilities in place to monitor connections, external service providers, devices and software.	New and/or malicious connections within the monitored environments are immediately viewable on Illumio's application dependency map. Output relating to these connections can be sent out to technologies such as a SIEM for further alerting and enrichment. Detail around the connection down to process level is available in this output for additional context, including role, application, environment, and location. These can include connections via APIs to other financial services, such as those used in the Payment Services Directive 2 (PSD2) or Open Banking.

EXPECTATIONS – "ADVANCING"	HOW ILLUMIO CAN HELP
The FMI should have the capabilities, in collaboration with other stakeholders, to detect cyber events and adapt its security controls swiftly. Such events may include attempted infiltration, movement of an attacker across systems, exploitation of vulnerabilities, unlawful access to systems and exfiltration of information or data.	The whitelisting policy model within Illumio ASP means that new attempted network connections are default-denied implicitly when the platform is running in the "enforced" mode. Any new flows can be sent out by means of feeds or taken as event data, allowing relevant systems to alert against attempts at lateral movement or compromise on the network. Built-in functionality around anti-tampering and auto-quarantining prevents compromise of Illumio ASP components on hosts themselves, and isolates systems if they are seen to be behaving in a malicious fashion.
The FMI should continuously monitor and inspect the network traffic, including remote connections, and end point configuration and activity to identify potential vulnerabilities or anomalous events in a timely manner.	Critical applications, environments, and workloads can be closely monitored for new, out-of-policy connectivity and output to other systems for analysis; or quarantined directly using Illumio's micro-segmentation functionality. With the ability to feed into upstream components such as SIEM technologies, and a full documented API for Illumio ASP, output on new or malicious connections can be correlated against; security posture and segmentation policies change dynamically based on attack information and vulnerability data.
The FMI should compare the network traffic and the end point configuration with the expected traffic and configuration baseline profile and data flows.	Illumio's real-time application dependency map allows a normal baseline of connectivity and network traffic to be established, both within applications and across environments. Simple green lines (allowed traffic) and red lines (disallowed traffic) indicate the network flows. Feeding new connection information from Illumio ASP in correlation technologies such as a SIEM allows comparison to threat intelligence information, vulnerability data, and attack vector simulation. A compromised workload will appear immediately in Illumio's application dependency map view with new attempted network connections clearly highlighted. In addition, process information tied to these network connections is also fed back into the system and upstream components for further investigation.

2.6 TESTING

This chapter of the Guidance provides guidance on areas that should be included in an FMI's testing and how results from testing can be used to improve the FMI's cyber resilience posture on an ongoing basis. The scope of testing for the purpose of this guidance includes vulnerability assessments, scenario-based testing, penetration tests and tests using red teams.

EXPECTATIONS – "EVOLVING"	HOW ILLUMIO CAN HELP
The FMI's vulnerability management process should help any type of exploitable weakness to be identified (technical, processual, organisational and emergent) in the critical functions, their supporting processes and information assets where they reside.	Illumio ASP can take in vulnerability data and map it to network port exposure, defining micro-segmentation policies in response to prevent exploitation of vulnerabilities before patches can be applied. The combination of vulnerability data and network flow mapping allows vulnerability-exposure scores to be calculated as a combination of how severe vulnerabilities are, where they are present, and how connected are the hosts the vulnerabilities present themselves on; as pertains to the leverageable ports themselves. Finally, policy can be created in response to the vulnerability exposure to reduce or stop communication into known vulnerable ports while still allowing necessary application traffic to flow.

As you can see, gaining visibility into and control of connections and flows inside of essential networks by means of a micro-segmentation solution is key to the SIPS guidance.

GETTING STARTED: VISIBILITY IS KEY TO ENFORCEMENT

How do you get started? Real-time visibility of traffic flows and potential compromises is an essential first step – after all, you can't protect what you can't see. Once a real-time application dependency map is established to view communication flows, it can then be used to derive granular policy and reporting. This exercise can also facilitate discovering and segmenting large areas of the sensitive network away from corporate IT as required. As the IT and OT (Operational Technology) worlds merge, tight control of the boundaries is needed. The Illumio Adaptive Security Platform provides the visibility and enforcement needed to adhere to the SIPS Guidance.

KEY BENEFITS:

- **See all your application dependencies and vulnerabilities** through Illumination®, a real-time traffic map.
- **Take control of lateral (East-West) traffic** within your data centre – ensuring that an attacker cannot move freely within your data centre or cloud.
- **Stop breaches in their tracks** by turning every host in your data centre and public cloud into a sensor that detects unauthorised traffic and an enforcement point for micro-segmentation policy.
- **Secure connectivity** within and between clouds and private data centres with policy-based IPsec encryption.
- **Eliminate service delivery delays** and deploy applications with security that operates at the speed of DevOps.
- **Write natural language policies** that Illumio ASP turns into IP-based enforcement rules.

KEY FEATURES:

- **Real-time maps** that display application traffic combined with existing vulnerability data.
- **Activation and management of existing enforcement points** delivers enforcement by activating the existing stateful firewalls in every host (with no kernel modifications), programming ACLs into load balancers, existing switches, and cloud provider security groups.
- **Automated policy recommendations** based on historical traffic flows that ensure micro-segmentation policies do not break applications.
- **Automated adaptive enforcement** that ensures optimal security remains intact as your applications scale or move and as new versions are deployed or old versions are decommissioned.

- **Policy-based encryption of data in motion** with AES-256 IPsec encryption between any mix of Linux/Windows workloads using transport mode and termination on VPN devices using tunnel mode.
- **Support for any underlying infrastructure** – new or existing environments with bare-metal, virtualisation, or containers on-premises, in the cloud, or across hybrid deployments.
- **Policy modeling and enforcement** on a workload, application, or environmental basis rather than on a hypervisor, VLAN, or security group basis.

ABOUT ILLUMIO

Illumio, the leader in micro-segmentation, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information about Illumio, visit www.illumio.com/what-we-do or follow @Illumio.

- Engage with Illumio on Twitter
- Follow Illumio on LinkedIn
- Like Illumio on Facebook
- Subscribe to the Illumio YouTube Channel

CONTACT US

For more information about Illumio ASP and how it can be used to achieve visibility behind the firewall, email us at illuminate@illumio.com or call 855-426-3983 to speak to an Illumio representative.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 www.illumio.com