Information Asset Inventory

International Networks at Indiana University
TransPAC, NEA3R

Updated: 09/1/2021

Authors: International Networks at Indiana University Staff
Information Security Officer: Hans Addleman

Table of Contents

Introduction

This document represents the International Networks at Indiana University's (IN@IU) authoritative inventory of information assets (i.e., information and information systems) as of the version date for the purposes of information security. Section 1 contains an inventory of IN@IU's information organized by information type. Section 2 contains an inventory of information systems. Both Sections 1 and 2 contain summary information regarding the security objectives (confidentiality, integrity, availability) relevant to each asset or type of asset. Section 3 provides additional descriptive details regarding key information assets. Section 4 contains listings of related resources and helpful figures.

Unlike policy documents, which may be reviewed infrequently, this inventory must be kept up to date to remain relevant and useful. Ideally, it should be updated every time there is a change in any of the information listed. This has proven to be lower-overhead than doing a monthly or quarterly inventory to update the documentation.

IN@IU maintains a data classification guide based in part on Indiana University's data classification guide. For information regarding violations and enforcement, please refer to the appropriate Master Information Security Policies & Procedures document for the project located at https://internationalnetworks.iu.edu/about/policies.html. You can find data classifications at the following URL: https://datamgmt.iu.edu/types-of-data/classifications.php.

1. Information Inventory

***Information* is any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.**

1.1 Personally Identifiable Information

Personally Identifiable Information (PII) is defined as any data that may be used to identify a person specifically. Examples include home phone numbers, addresses, social security addresses, or passwords.

Asset Name	Short Description	Owner	Information Classification	Associated Project
Team Internal Contact Info	Phone numbers, home and work addresses, and email addresses. May be stored in multiple places including personal contacts and the GlobalNOC database.	Team	University-Internal	
Team External Contact Info	Public Contact information for our team including group email addresses and lists.	Team	Public	
Partner Contact Database	Tracked in Trello.	Team	University-Internal	
Chat logs	Slack and other instant message (IM) clients may store local logs on laptops, phones, and tablets. The IM server may also store chat logs.	Team	University-Internal	

Email	Email stored server side and of laptops of the team may contain sensitive PII. Email servers are tracked in the Information Systems section of this document.	GlobalNOC /IU-UITS	University-Internal	
Netflow Records	Netflow records gathered from our switches and routers contain a wealth of information that can identify a single user and their destination. This information is critical and should never be shared outside of the team.	Team	Critical	TransPAC, NEAAR
Root Passwords File	A secure text file of passwords used for root and system level access to IN@IU resources.	GlobalNOC	Critical	TransPAC, NEAAR

Confidentiality: All PII must be kept confidential, distributed on a need-to-know basis only.
Integrity: The integrity of PII is important, but no more so than with other data we manage.
Availability: While availability of all project data is important, the only PII that absolutely must be accessible at all times in a disaster is staff emergency contact information, device root passwords, one time tokens, and building access badges. Permanent loss of PII would be costly and potentially embarrassing to the project, however, loss of availability is preferable to loss of confidentiality given the sensitive nature of the data.

1.2 Network Telemetry

1.2.1 Public Network Telemetry

This data entails anything collected from our network devices for research, troubleshooting, or operations not including data that may contain PII or critical configuration files.

Asset Name	Short Description	Owner	Information Classification	Associated Project
Routing Tables	Daily internet routing tables gathered from IN@IU owned routers	Hans Addleman	Public	TransPAC
SNMP Data	Simple Network Management Protocol data from network devices. This includes port up/down, device up/down, and interface traffic/error statistics.	GlobalNOC	Public	TransPAC, NEAAR

Confidentiality: Public Network Telemetry is not generally considered confidential. Some of the information can be accessed by the public on IN@IUMay web pages (such as the Router Config Proxy). Information that is not on the website may be requested via the IRNC NOC.

Integrity: Integrity of this information is important for historical and troubleshooting exercises. Corrupt data could lead to poor reporting or longer lead times troubleshooting network issues.

Availability: This stored data should be generally available. It is used for troubleshooting on a day to day basis.

1.2.2 Non Public Network Telemetry

This is network equipment and server configuration data used for configuration replication and forensics.

Asset Name	Short Description	Owner	Information Classification	Associated Project
Network Device Configs	Configuration files with change tracking stored on a server. These files are stored with all sensitive data removed. IE: passwords and keys	GlobalNOC	University Internal	TransPAC, NEAAR
Network Device Logs	Log messages generated by network devices sent via syslog protocol to servers for storage and use.	GlobalNOC	University Internal	TransPAC, NEAAR

Confidentiality: (something about non public network telemetry) Device configurations are not generally considered confidential. Some of the information can be accessed by the public on TransPAC or NEAAR web pages (such as the Router Config Proxy). Information that is not on the website may be requested via the IRNC NOC.

Integrity: Integrity of this information must be maintained in case of device failure and the need to quickly replicate configurations.

Availability: The stored configuration data should be accessible at all times in case of emergency need.

1.3 Publicly Shared Information

This category encompases documents and information that we publically share.

Asset Name	Short Description	Owner	Information Classification	Associated Project
MOU's	Memorandums of Understanding between International Networks and our Partners.	Team	Public	
Presentations	Presentations created, maintained, or disseminated by the team. These should not contain sensitive information.	Team	Public	
Network diagrams	Diagrams and drawings of network topologies and designs. These should not contain IP addresses.	Team	Public	
Public Reports	These are the quarterly, yearly, and final reports that are posted to our public websites. Sensitive information including financials has been removed.	Team	Public	
perfSONAR data	perfSONAR MaDDash information	Team	Public	

Confidentiality: This data has no requirement of confidentiality and can be freely shared.

Integrity: This type of information should be as accurate as possible as it is shared with the outside world. It would be an embarrassment to the team if the information was corrupt.
Availability: It is not critical for this data to be always accessible. It can be requested on an as needed basis from a tape, drive, or cloud backup.

1.4 Internal Team Information

This is information that we share internally with our group. It is generally not for public consumption. This information may contain PII, however, in which case it should not be anything more than an individual's name and organization.

Asset Name	Short Description	Owner	Information Classification	Associated Project
Draft MOUs		Team	IU-Internal	
Network diagrams with non public information	Network maps and diagrams depicting current, upcoming, and proposed configurations. These may contain sensitive information such as management IP addresses, etc.	Team	IU-Internal	
NSF Reports	These are the quarterly, yearly, and final reports that are posted to our public websites. These reports add in the project financial information for that time period and should only be submitted to the NSF.	Team	IU-Internal	
Trello Task Manager	This cloud based service tracks our ongoing tasks and projects.	Team	IU-Internal	

Contracts	Contracts and agreements with vendors. May contain budgetary or other proprietary data.	Team	Critical	
Notes	Team members take meeting and work notes both physically and electronically in programs like Evernote and Apple Note.	Team	IU-Internal	

Confidentiality: This information is not confidential, however, team members should check with security officer or manager before sharing.

Integrity: Integrity is not critical, however, care should be taken as these are resources that are used daily.

Availability: Availability is of highest importance as this information is used daily by the team.

2 Information Systems Inventory

An *information system* is a discrete set of information and related resources (such as people, equipment, and information technology) organized for the collection, processing, maintenance, use, sharing, dissemination, and/or disposition of information.

2.1 Computer, Phone, and Mobile Devices

Both personal and work mobile devices and desktops are in this category. Any device used to access TransPAC or IU resources should follow the guidelines presented by the IU Security and Policy offices.

Asset Name	Short Description	Owner	Asset Detail / Policy	Associated Project
Personnel-Owned phones	Typically used for 2FA (two factor authentication) and email.	Individual	https://protect.iu.edu/online-safety/policies/it121.html	
IU owned Computers	Ongoing work related and incidental personal use.	Individual	https://protect.iu.edu/online-safety/policies/it121.html	
Personnel Owned Computers	Privately owned computer or laptop that may be used for access to IN@IU systems.	Individual	https://protect.iu.edu/online-safety/policies/it121.html	

Confidentiality: Mobile phones, laptops, and desktops are likely to contain confidential information such as soft tokens for 2fa, email, database access, and more.

Integrity: Integrity concerns are limited to issues such as malware that might compromise the confidentiality of information stored on or transmitted to/from mobile devices. Soft tokens and other authentication credentials can be revoked and reissued, copies of email and other data accessed via mobile devices are stored elsewhere and can be restored or verified per our Disaster Recovery Policy.

Availability: Unavailability of mobile devices and laptops may cause a user to be unable to complete a 2FA challenge and log in to systems. It may also cause slower response times, lost work time, and possibly lost information if not backed up centrally.

2.2 GlobalNOC / Indiana University Managed Servers with possible PII

These servers or services are managed by the Indiana University GlobalNOC or Indiana University UITS teams. They are covered by their respective owners' policies. IN@IU personnel are users of these servers.

Asset Name	Short Description	Owner	Asset Detail	Associated Project
Exchange	Exchange email and calendaring services are managed and secured by UITS with policies mandated by UISO.	UITS	https://kb.iu.edu/d/agxv	
Slack Instances	Instant Messenger service managed by GlobalNOC and UITS	GlobalNOC	https://globalnoc.iu.edu/	

Confidentiality: These servers may contain PII including names, email addresses, phone numbers, physical addresses, and other non critical PII.

Integrity: A compromised mail or chat server could be used for a number of malicious purposes including spam.

Availability: Mail and chat servers should be constantly available and loss of availability can decrease productivity drastically. These servers must have hot backup and quick restoration capabilities as they hold tools and data used daily by the TransPAC NOC and Network Engineering.

2.3 GlobalNOC / Indiana University Managed Servers without PII

These servers or services are managed by the Indiana University GlobalNOC or Indiana University UITS teams. They are covered by their respective owners' policies. IN@IU personnel are users of these servers.

Asset Name	Short Description	Owner	Asset Detail	Associated Project
GlobalNOC Database	The GlobalNOC database is used for storing information on Network Devices, colocation facilities,circuit information, and contact information.	GlobalNOC	https://db2.grnoc.iu.edu/grnocdb2/	
Telemetry Collectors	Servers used for the collection of network telemetry including but not limited to RANCID, Syslog, SNMP, and netflow	GlobalNOC		
perfSONAR servers	IN@IU has a perfSONAR host in Seattle that is publically available for testing.	GlobalNOC		

Confidentiality: N/A

Integrity: Servers in this category must be protected as the data they house data directly related to the ongoing operation of the TransPAC network.

Availability: These servers must have hot backup and quick restoration capabilities as they hold tools and data used daily by the TransPAC NOC and Network Engineering.

2.4 International Networks Equipment

These assets are servers and network equipment used in International Networks deployments in support of the TransPAC and NEAAR projects. They are operated and managed on IN@IU's behalf by the IU GlobalNOC.

Asset Name	Location	Short Description	Owner	Asset Detail	Associated Project
Arista 7280	New York	An Arista router that provides peering services.	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=32142	NEAAR
Dell R630	New York	PerfSONAR server	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=24327	NEAAR
Cisco 2921	New York	Out of Band Router	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=24286	NEAAR
Servertech Sentry DC PDU	New York	Servertech Sentry Networked DC power distribution unit	Team	https://db2.grnoc.iu.edu/grnocdb2/?meth	NEAAR

				od=node_details&node_id=24345	
Tripplite AC PDU 1 - Decommissioned	Storage/Pod3	Networked AC power distribution unit	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=29402	TransPAC
Tripplite AC PDU 2 - Decommissioned	Storage/Pod3	Networked AC power distribution unit	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=29407	TransPAC
Cisco 2921 - Decommissioned	Storage/Pod3	Out of Band Router	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=29412	TransPAC
Dell R330 - Decommissioned	Storage/Pod3	PerfSONAR server	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=28202	TransPAC
Dell R640 - Decommissioned	Storage/Pod3	Netsage probe - Managed by GlobalNOC	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=28257	Netsage / TransPAC

Dell R740xd - Decommissioned	Storage/Pod3	A test file transfer node that will be used for production services - Managed by GlobalNOC	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=28237	TransPAC
Arista 7280 - Decommissioned	Storage/Pod3	An Arista Router used for production peering in Hong Kong. - Managed by GlobalNOC	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=29397	TransPAC
Brocade MLXe-4	Seattle	A Brocade switch in production for the TransPAC network. - Managed by GlobalNOC	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=20431	TransPAC
Cisco 2921	Seattle	Out of band router - Managed by GlobalNOC	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=20419	TransPAC
Dell R630	Seattle	TransPAC perfSONAR server - Managed by GlobalNOC	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=20209	TransPAC
ServerTech 4805	Seattle	Servertech 4805/35-XLS-12 DC Power Controller. - Managed by GlobalNOC	Team	https://db2.grnoc.iu.edu/grnocdb2/?method=node_details&node_id=20425	TransPAC

Confidentiality: N/A

Integrity: No code or data should not be stored long term.

Availability: These test devices should only be reachable via the secured management network when they are available.

2.4 International Networks test and lab equipment

These assets are servers and network equipment used in use the IN@IU Lab or test environment.

Asset Name	Location	Short Description	Owner	Asset Detail	Associated Project
Ixia Tester	Moveable (currently in IUB Datacenter Storage)	A 100G network tester that can be moved around the world and loaned to partners for testing and validation of high speed links.	Team	https://www.ixiacom.com	
Viavi Tester	Moveable (Currently in Guam)	A 2x100G hand held Test set.	Team		
SuperMicro half-depth 1RU	Rack 01.04	thrpt10ge-1.in.iu.edu (149.165.239.227) CentOS 7; pS 4.1.x Behind GlobalNOC bastion hosts and auto-updated via perfSONAR Toolkit	Doug		perfSONAR

Confidentiality: N/A

Integrity: These are all test hosts and any code or data should not be stored long term.

Availability: These test devices should only be reachable via the secured management network when they are available.

***

This document is based in part on CTSC Information Asset Template, v2.
For template updates, visit trustedci.org/guide.