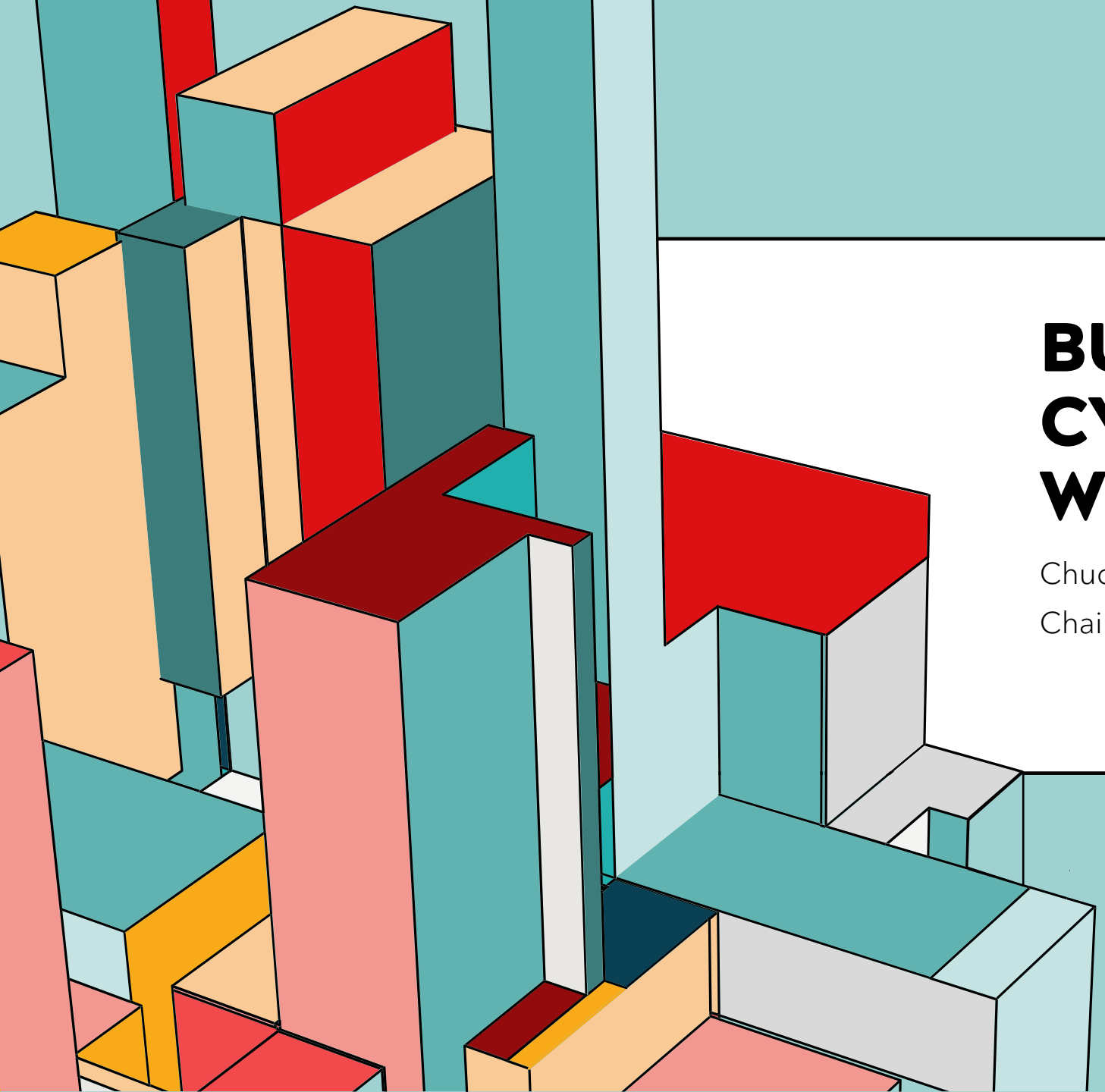


BUILDING A CYBERSECURITY WORKING GROUP

Chuck Mitchell, Commerce OIG

Chair of the CIGIE Cybersecurity Working Group

CYBERSECURITY IS HARD

LEARNING OBJECTIVES

Vision

Structure

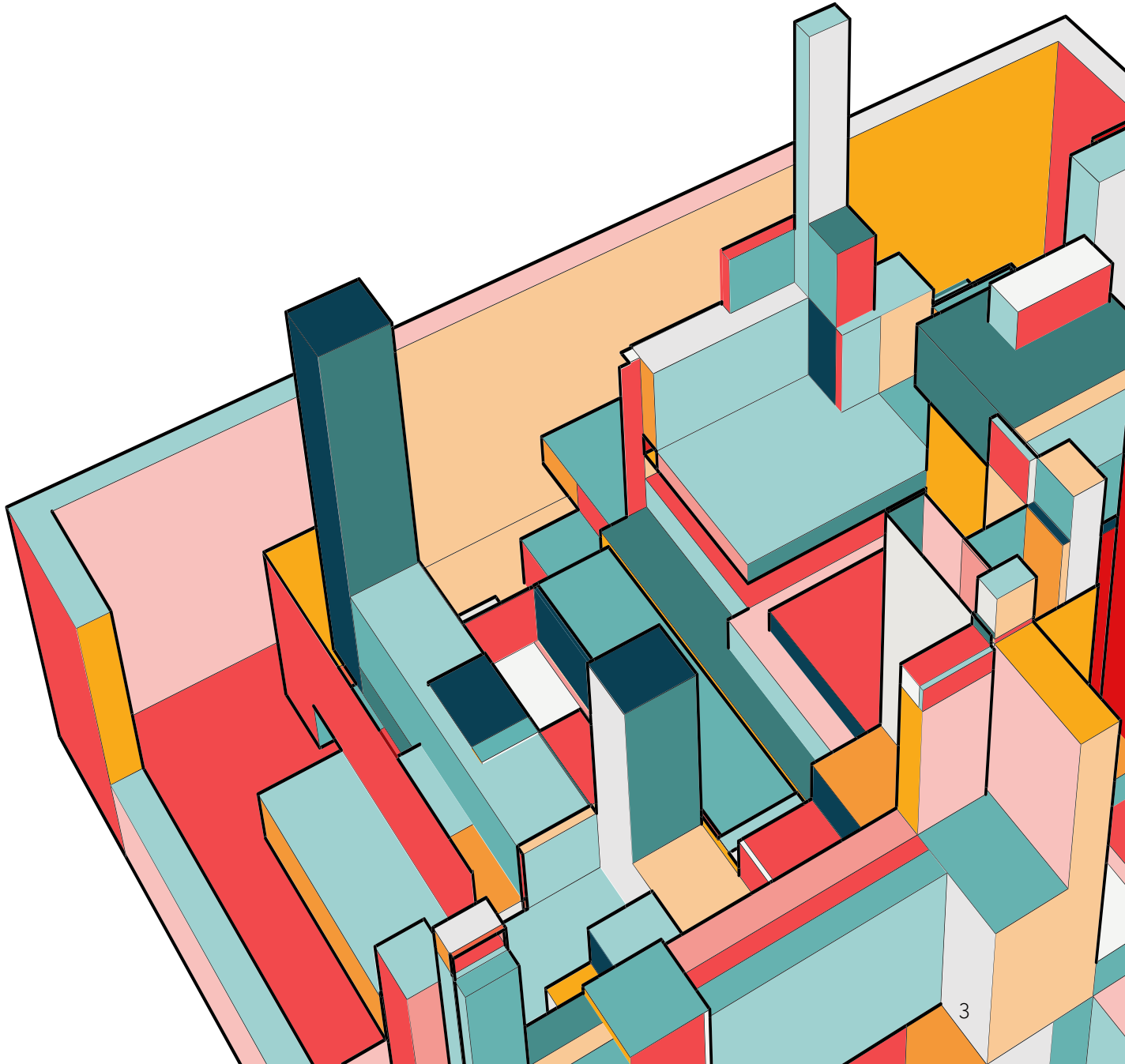
Initiatives

Progress

People

Challenges

Momentum



WHERE TO START

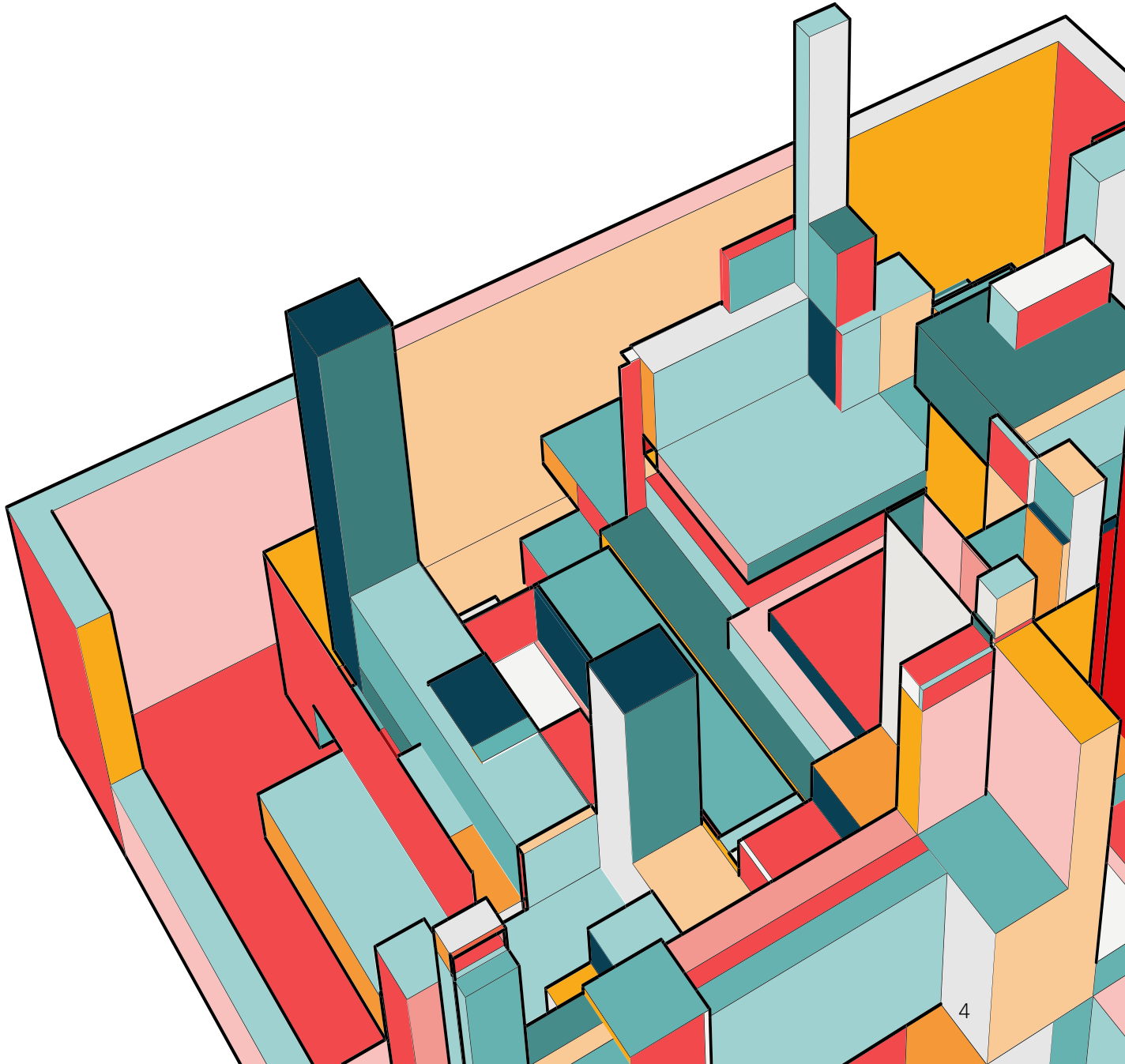
People are interested

Put out a call

Hold an information session

Ask people what they want

Set the vision

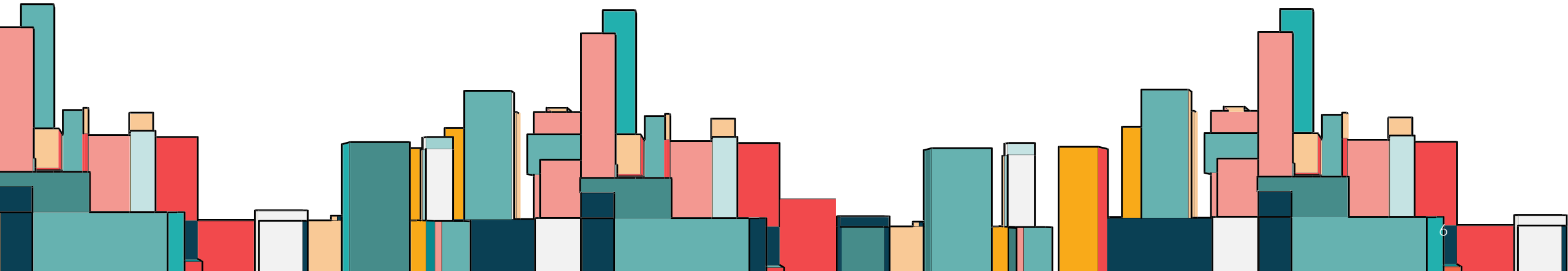


POLL #1 – WHAT IS YOUR LEVEL OF CYBERSECURITY EXPERTISE?

1	2	3
Specialist / Primary Job Duty	Not an expert but I'm familiar with the concepts	Annual training and that's about it

VISION

Raise the overall understanding of cybersecurity across the OIG community



STRUCTURE THE TEAM

Chair

Motivated, labour of love

Vice Chair

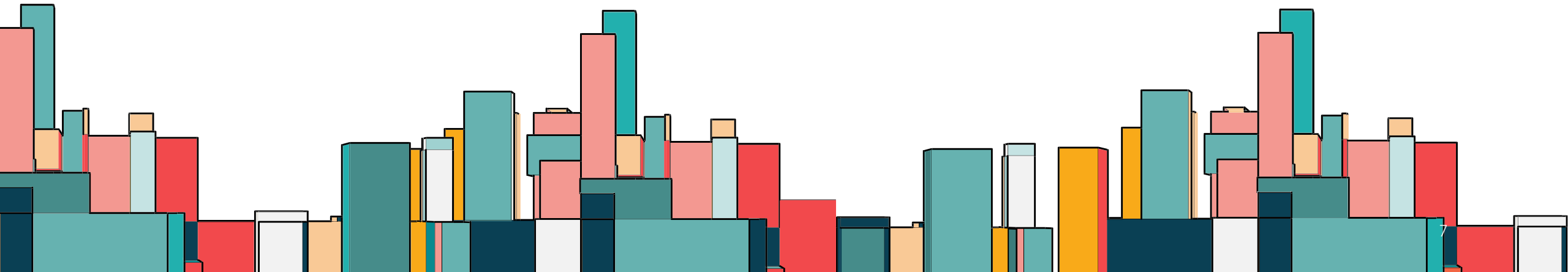
Connected, ready to help

Leads

First to volunteer, wants to make a difference

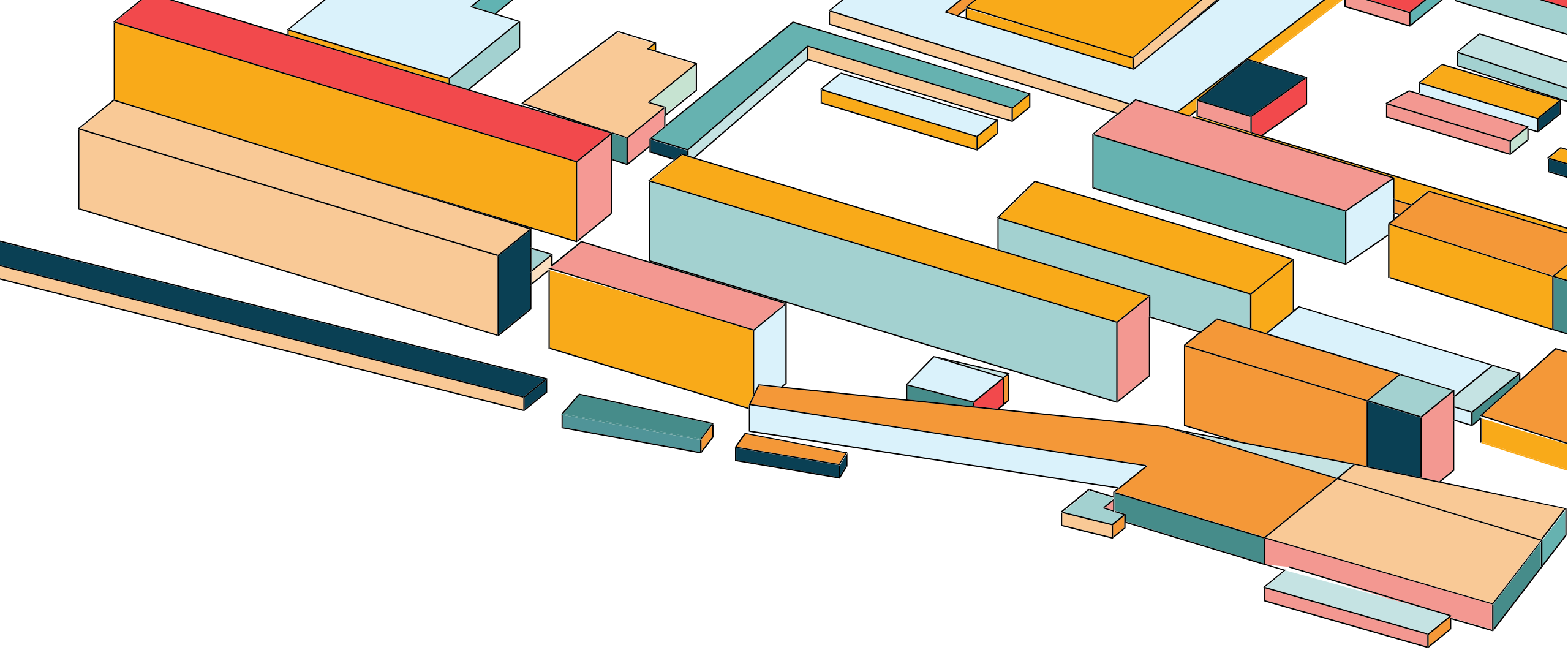
Volunteers

Interested, willing to pitch in if asked



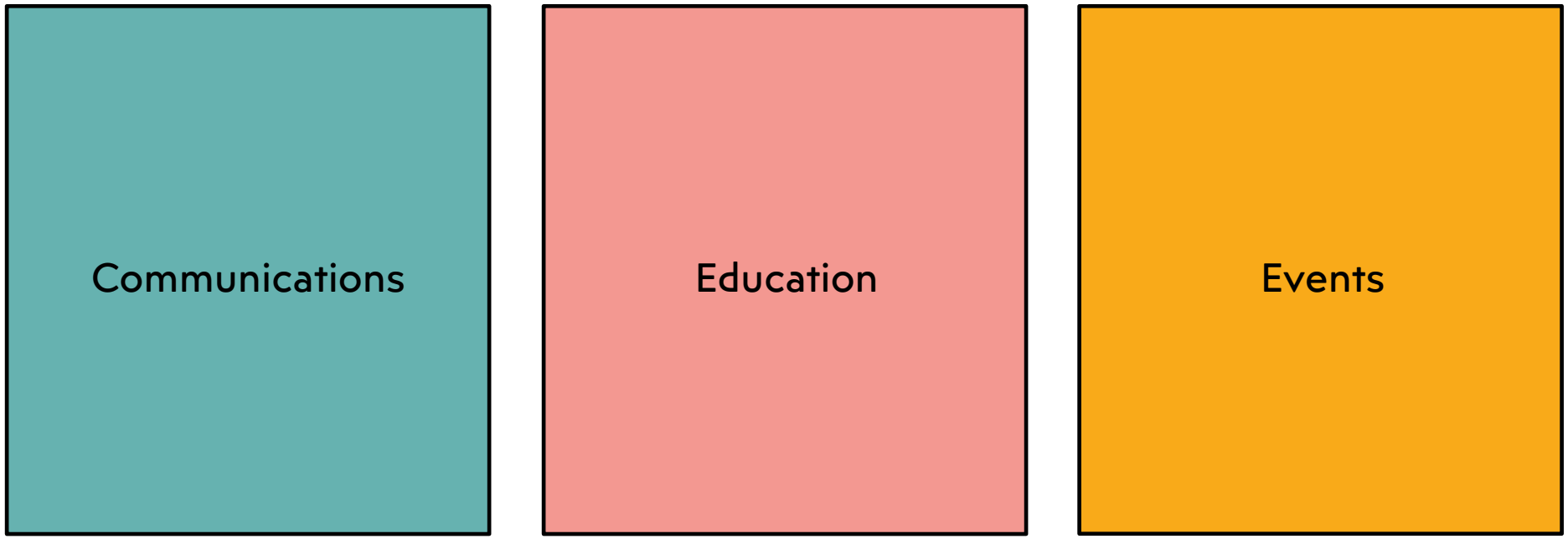
POLL #2 – WHAT LEVEL WOULD YOU PARTICIPATE AT?

1	2	3
Lead the charge	Pitch in where I can	Listen in to stay informed



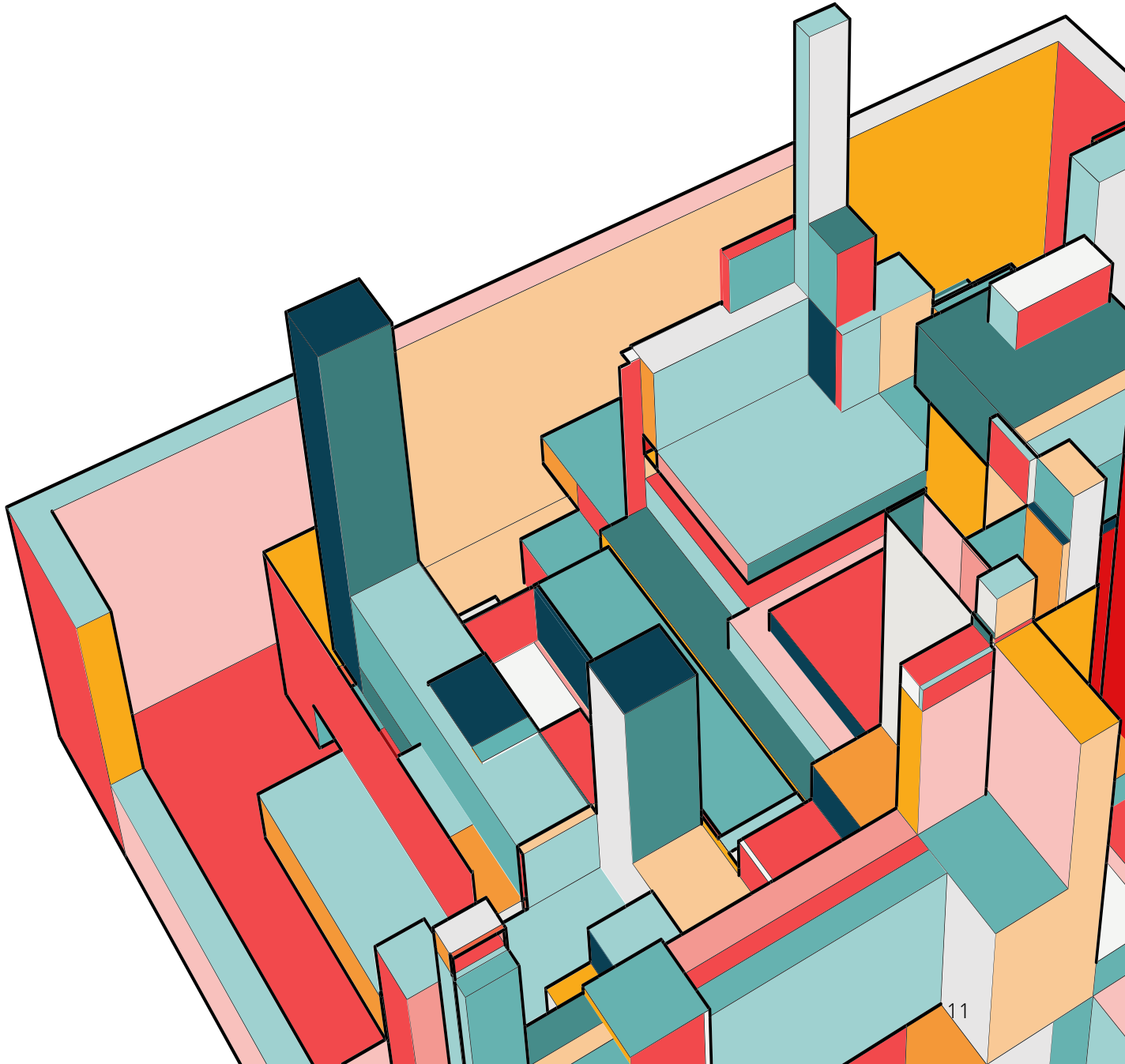
ESTABLISH INITIATIVES

OUR INITIATIVES



COMMUNICATIONS

Goal: Keep the OIG community current on cybersecurity news / events / guidance and serve as a touch point throughout CIGIE.



COMMUNICATIONS TASKS

Detailed Newsletter

Fortnightly to a broad audience

Executive Newsletter

Monthly to Inspectors General

Design + Engage

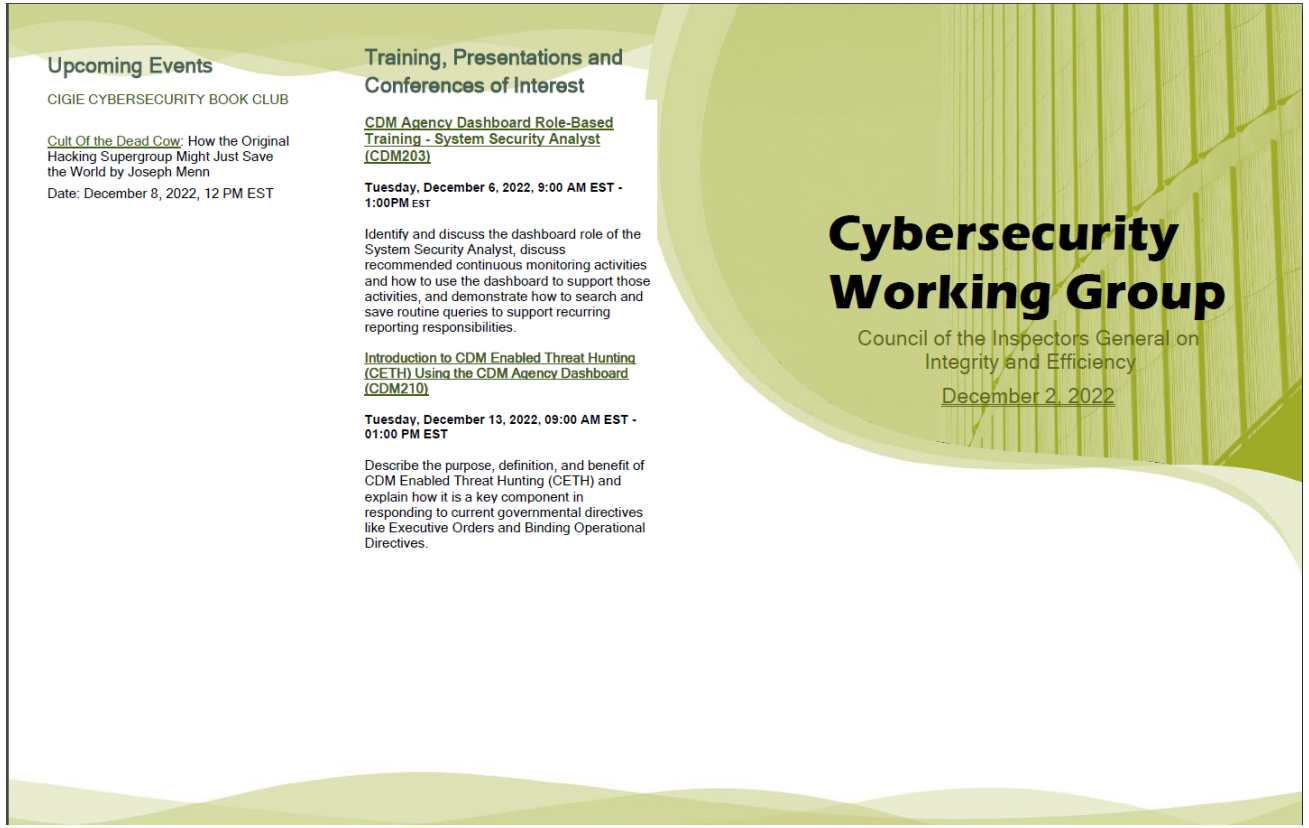
Design an overall coms strategy

Stay in touch

DETAILED NEWSLETTER

Sections:

- Upcoming Events
- Job Postings
- Training, Presentations, and Conferences of Interest
- Security Hot Topics
- Cybersecurity Audits and Evaluations
- Recent Attacks
- Binding Operational Directives (BODs), Executive Orders, Office of Management and Budget Memorandums
- CISA Alerts and Vulnerabilities



Upcoming Events

CIGIE CYBERSECURITY BOOK CLUB

Cult Of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World by Joseph Menn

Date: December 8, 2022, 12 PM EST

Training, Presentations and Conferences of Interest

CDM Agency Dashboard Role-Based Training - System Security Analyst (CDM203)

Tuesday, December 6, 2022, 9:00 AM EST - 1:00PM EST

Identify and discuss the dashboard role of the System Security Analyst, discuss recommended continuous monitoring activities and how to use the dashboard to support those activities, and demonstrate how to search and save routine queries to support recurring reporting responsibilities.

Introduction to CDM Enabled Threat Hunting (CETH) Using the CDM Agency Dashboard (CDM210)

Tuesday, December 13, 2022, 09:00 AM EST - 01:00 PM EST

Describe the purpose, definition, and benefit of CDM Enabled Threat Hunting (CETH) and explain how it is a key component in responding to current governmental directives like Executive Orders and Binding Operational Directives.

Cybersecurity Working Group

Council of the Inspectors General on Integrity and Efficiency

December 2, 2022

Cybersecurity Working Group

Council of the Inspectors General on Integrity and Efficiency

December 2, 2022

Upcoming Events

CIGIE CYBERSECURITY BOOK CLUB

Cult Of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World by Joseph Menn

Date: December 8, 2022, 12 PM EST

Job Board

Training, Presentations and Conferences of Interest

CDM Agency Dashboard Role-Based Training - System Security Analyst (CDM203)

Tuesday, December 6, 2022, 9:00 AM EST - 1:00PM EST

Identify and discuss the dashboard role of the System Security Analyst, discuss recommended continuous monitoring activities and how to use the dashboard to support those activities, and demonstrate how to search and save routine queries to support recurring reporting responsibilities.

Introduction to CDM Enabled Threat Hunting (CETH) Using the CDM Agency Dashboard (CDM210)

Tuesday, December 13, 2022, 09:00 AM EST - 01:00 PM EST

Describe the purpose, definition, and benefit of CDM Enabled Threat Hunting (CETH) and explain how it is a key component in responding to current governmental directives like Executive Orders and Binding Operational Directives.

Security Hot Topics

It's Time for Better Data Protection: Why the 3-2-1 Rule Isn't Enough

Data has become a critical resource that's central to keeping operations running. So, when ransomware causes a business to lose access to its data, operations can become paralyzed for days or weeks. It's at this point that many organizations that are still reliant on 3-2-1 approaches discover that their recovery isn't fast and won't necessarily be guaranteed. Organizations looking to build on their traditional 3-2-1 strategy are now turning to Disaster Recover as a Service (DRaaS) providers that offer the hosted infrastructure resources, data replication and continuous data protection technologies they need to maintain critical data resilience and recoverability across all their environments -- on-premises, hybrid and multi-cloud.

U.S. Military Goes Zero-Trust on Software and Government Gets Busy

The Pentagon this week outlined its zero-trust strategy roadmap. The Department of Defense wants to put a zero-trust framework fully in place by 2027, and the strategy encompasses four goals that include ensuring that personnel are aware of and trained for zero trust and that it covers all information systems.

Augmenting Supply Chain Resilience Through Unified Endpoint Management

Cybersecurity must be an integral part of your supply chain strategy. However, cybersecurity is a vast realm involving many domains. Owing to the significant increase in the use of mobile and IoT devices, securing and managing the plethora of endpoints deployed in your fleet through unified endpoint management (UEM) solutions is a great launching point to improve cyber resilience.

Cybersecurity Audits/Evaluations

DoD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents are Appropriately Reported and Shared

GAO issued a report this week that made six recommendations to DOD. Recommendations included assigning responsibility for ensuring proper incident reporting, improving the sharing of DIB-related cyber incident information, and documenting when affected individuals are notified of a PII breach. DOD concurred with the recommendations

Recent Attacks

Microsoft Attributes Alleged Chinese Attack on Indian Power Grid to "Boa" IoT Vulnerability

Microsoft has tied an attack on seven facilities managing the electricity grid in Northern India to a vulnerability affecting a web server discontinued in 2005 but still used widely by vendors across a variety of IoT devices and popular software development kits. Microsoft noted that the attacks were part of a string of attacks on Indian critical infrastructure since 2020 that has continued until as recently as October 2022, when the Hive ransomware group attacked major energy provider Tata Power.

EU Parliament Website Attacked After Members of Parliament Slam Russian 'Terrorism'

The European Parliament website was hit by a cyberattack claimed by pro-Russian hackers Wednesday shortly after lawmakers approved a resolution calling Moscow a "state sponsor of terrorism". The parliament website was targeted by a DDOS attack designed to force high levels of outside traffic onto the site's server, disrupting the network.

US Merit Systems Protection Board Compromised in Iranian Government-Linked Hack: Report

The U.S. Merit Systems Protection Board, responsible for arbitrating disputes with federal employees, was compromised in an Iranian government-linked hack earlier this year, according to a report. Hackers exploited the well-known Log4Shell vulnerability to install cryptocurrency mining software and compromise credentials, the Cybersecurity and Infrastructure Security Agency said Wednesday in an alert. It remains unclear what information may have been compromised because of the incident, but hackers broke into an unpatched VMware Horizon server in February and then used that access to move laterally within the network of an unidentified federal agency, according to the CISA alert.

Binding Operational Directives (BODs), Executive Orders, Office of Management and Budget Memorandums

Known Exploited Vulnerabilities (KEVs)

- 3 exploited vulnerabilities were due this week
- 5 exploited vulnerabilities are due week of December 9, 2022
- 2 exploited vulnerability issued this week. See details on page 3

Migrating to Post-Quantum Cryptography (PDF)

OMB memorandum M-23-02 provides direction for agencies to comply with the National Security Memorandum 10 in preparation for implementing post-quantum cryptography. Agencies must comply with the following deadlines:

- ✓ December 18, 2022, designate a cryptographic inventory and migration lead for their organization.
- ✓ May 4, 2023, and annually thereafter, agencies must submit a prioritized inventory of information systems and assets, excluding national security systems, that contain cryptanalytically relevant quantum computer (CRQC)-vulnerable cryptographic systems to the Office of the National Cyber Director and the Department of Homeland Security Cybersecurity and Infrastructure Security Agency.
- ✓ June 3, 2023, and annually thereafter, funding requirement assessment for migration.

National Cyber Awareness Systems Alerts

Title	Publication Date
AA22-335A: #StopRansomware: Cuba Ransomware	12/01/2022
AA22-321A: #StopRansomware: Hive Ransomware	11/17/2022
AA22-320A: Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester	11/16/2022
AA22-294A: #StopRansomware: Daixin Team	10/21/2022
AA22-279A: Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors	10/6/2022
AA22-277A: Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization	10/4/2022
AA22-265A: Control System Defense: Know the Opponent	9/22/2022
AA22-264A: Iranian State Actors Conduct Cyber Operations Against the Government of Albania	9/21/2022
AA22-257A: Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations	9/14/2022
AA22-249A: #StopRansomware: Vice Society	9/6/2022

National Cyber Awareness Systems Current Activity

Title	Publication Date
CISA and FBI Release Advisory on Iranian Government-Sponsored APT Actors Compromising Federal Network	11/16/2022
Mozilla Releases Security Updates for Multiple Products	11/16/2022
Samba Releases Security Updates	11/16/2022
Cisco Releases Security Updates for Identity Services Engine	11/16/2022
CISA Releases Two Industrial Control Systems Advisories	11/17/2022
#StopRansomware: Hive	11/17/2022
CISA, NSA, and ODNI Release Guidance for Customers on Securing the Software Supply Chain	11/17/2022
CISA Releases Eight Industrial Control Systems Advisories	11/22/2022
CISA Adds Two Known Exploited Vulnerabilities to Catalog	11/28/2022
CISA Releases Seven Industrial Control Systems Advisories	11/29/2022
CISA Releases Three Industrial Control Systems Advisories	12/1/2022
#StopRansomware: Cuba Ransomware	12/1/2022

CISA Known Exploited Vulnerabilities

CVE	Product	Date Added	Due Date
CVE-2022-4135	Chromium	11/28/2022	12/19/2022
CVE-2021-35587	Fusion Middleware	11/28/2022	12/19/2022

EXECUTIVE NEWSLETTER

Sections:

- In The News
- Cyber-Jargon
- Topics of Interest
- Recent OIG Work
- Important Dates

Cybersecurity Working Group

Council of the Inspectors General on Integrity and Efficiency

Executive Newsletter November 2022

IN THE NEWS

Biden Administration Unveils Cybersecurity Goals for Critical Infrastructure Operators

The Department of Homeland Security unveiled new benchmarks for critical infrastructure to strengthen cybersecurity defenses. The cybersecurity performance goals – developed by the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology – lays out the voluntary security steps the government expects all critical infrastructure entities to undertake.

Amid a Recent Wave of Layoffs Across the Technology Sector, the VA is Working to Position Itself as an Enticing Destination for Unemployed Tech Workers

With sweeping layoffs at major U.S. technology companies putting tens of thousands of highly skilled workers back into the job market in recent months, the Department of Veterans Affairs is working to entice talented tech employees to join the agency by conducting targeted outreach, launching an expanded career website, and working to expand pay for federal tech specialists.

CYBER-JARGON

- Quantum Computer - Machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or impossible for conventional computers.
- Qubit - a quantum bit, is the basic unit in quantum computing. Unlike a bit with just two states (0 or 1), a qubit can represent any proportion between 0 and 1, allowing a single qubit to represent significantly more values. Usings qubits, a quantum computer could break existing encryption in minutes instead of millions of years.
- Post-Quantum Cryptography (PQC) - An area of cryptography that researches and advances the use of quantum-resistant techniques, with the goal of keeping existing public-key encryption safe in the era of quantum computing.

TOPICS OF INTEREST

Red, Purple, and Blue -- Security Teams Keeping the Hackers at Bay

Regardless of how much money is spent on cybersecurity, the likelihood of getting hacked is steadily increasing as the threat landscape continues to evolve. Security software alone does not offer complete protection. A solution is to find your own weaknesses and remediate them before they can be exploited. One of the best ways to do this is through red, blue, and purple team testing.

RECENT OIG WORK (OVERSIGHT.GOV)

Simulated Internal Cyber Attack Gained Control of Critical Census Bureau Systems

The Department of Commerce OIG initiated the audit to determine the effectiveness of the U.S. Census Bureau's cybersecurity posture against a simulated real-world attack.

IMPORTANT DATES

Migrating to Post-Quantum Cryptography (PDF)

OMB memorandum M-23-02 provides direction for agencies to comply with the National Security Memorandum 10 in preparation for implementing post-quantum cryptography. Agencies must comply with the following deadlines:

- ✓ December 18, 2022, designate a cryptographic inventory and migration lead for their organization.
- ✓ May 4, 2023, and annually thereafter, submit a prioritized inventory of information systems and assets that contain relevant systems to the Office of the National Cyber Director and the Cybersecurity and Infrastructure Security Agency
- ✓ June 3, 2023, and annually thereafter, funding requirement assessment for migration.

There is a more detailed biweekly version of this newsletter available. Sign-up by emailing: <cmitchell@oig.doc.gov>

DESIGN + ENGAGE

Quarterly Focus

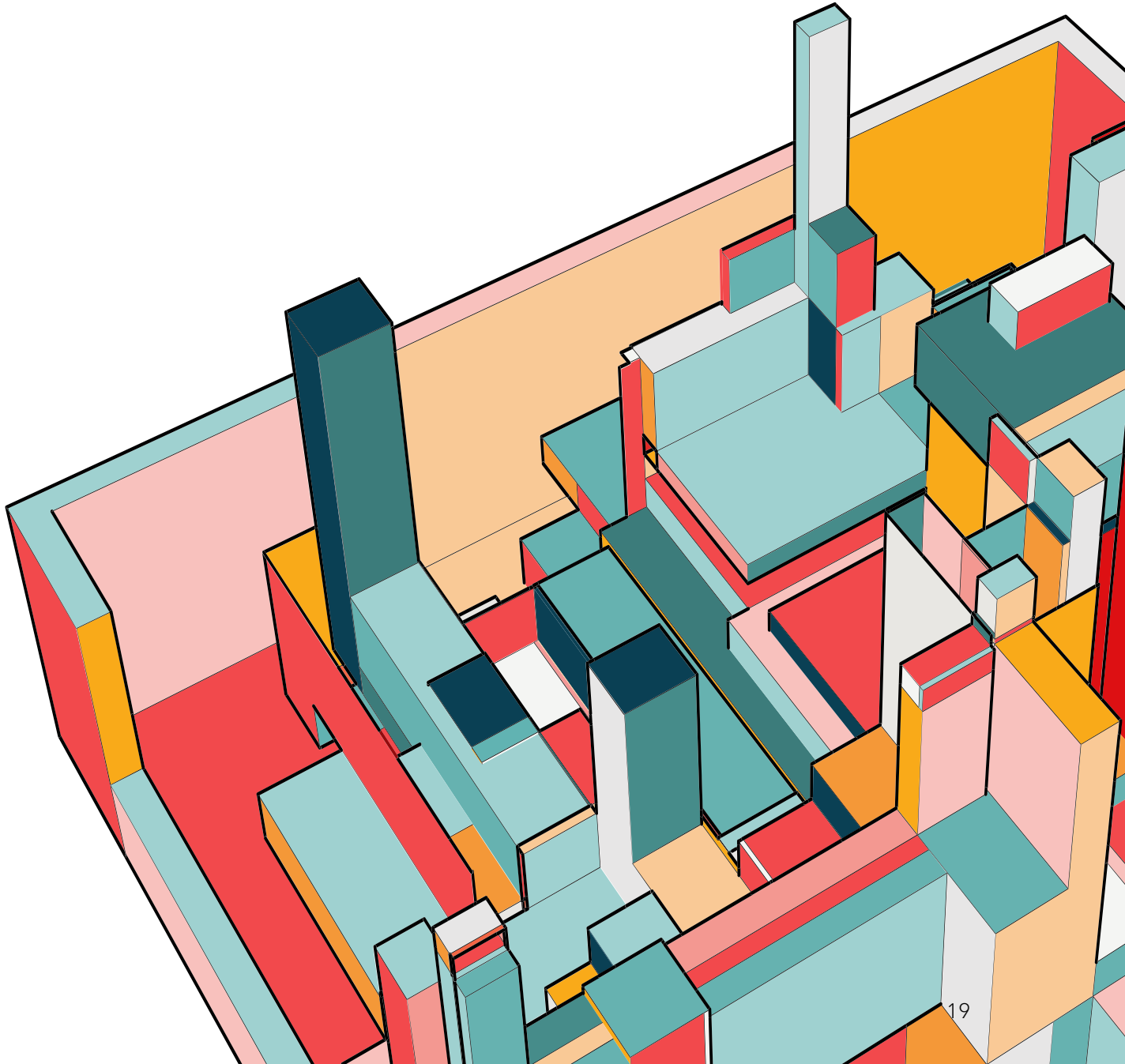
- New undertaking for the group
- Select a topic that all initiatives will focus on
- Benefit: Allows the team to focus and plan

Committee Outreach

- Get involved
- Listen to feedback and potential topics
- Get the word out with a personal touch

EDUCATION

Goal: Identify and coordinate delivery of formal training or educational talks that maintain and enhance the OIG community's cybersecurity skills.



POLL #3 – WHAT TYPE OF TRAININGS ARE YOU MOST INTERESTED IN?

1	2	3
Hands-on highly technical	Technical but lecture style	Less technical – bring me up to speed and keep it plain language

EDUCATION TASKS

Identify Topics

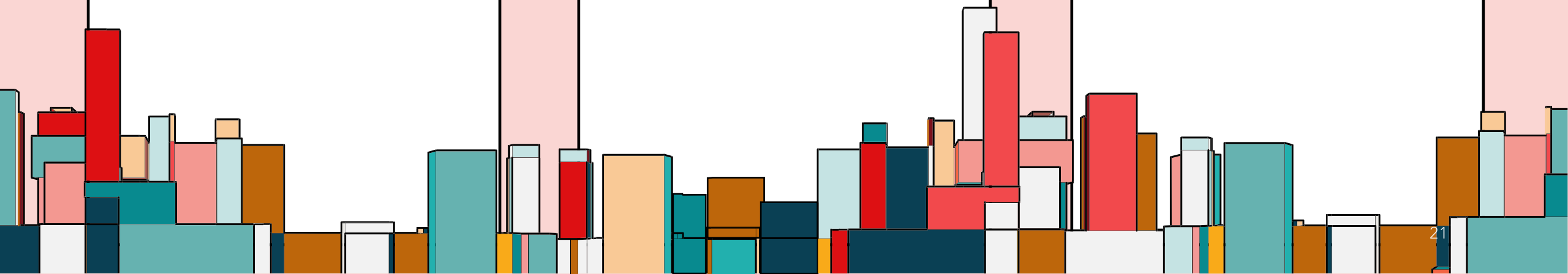
Zero Trust 101
Mobile and Cloud Forensics
CISA Vulnerability Disclosure Policy Platform
GSA FedRAMP Program

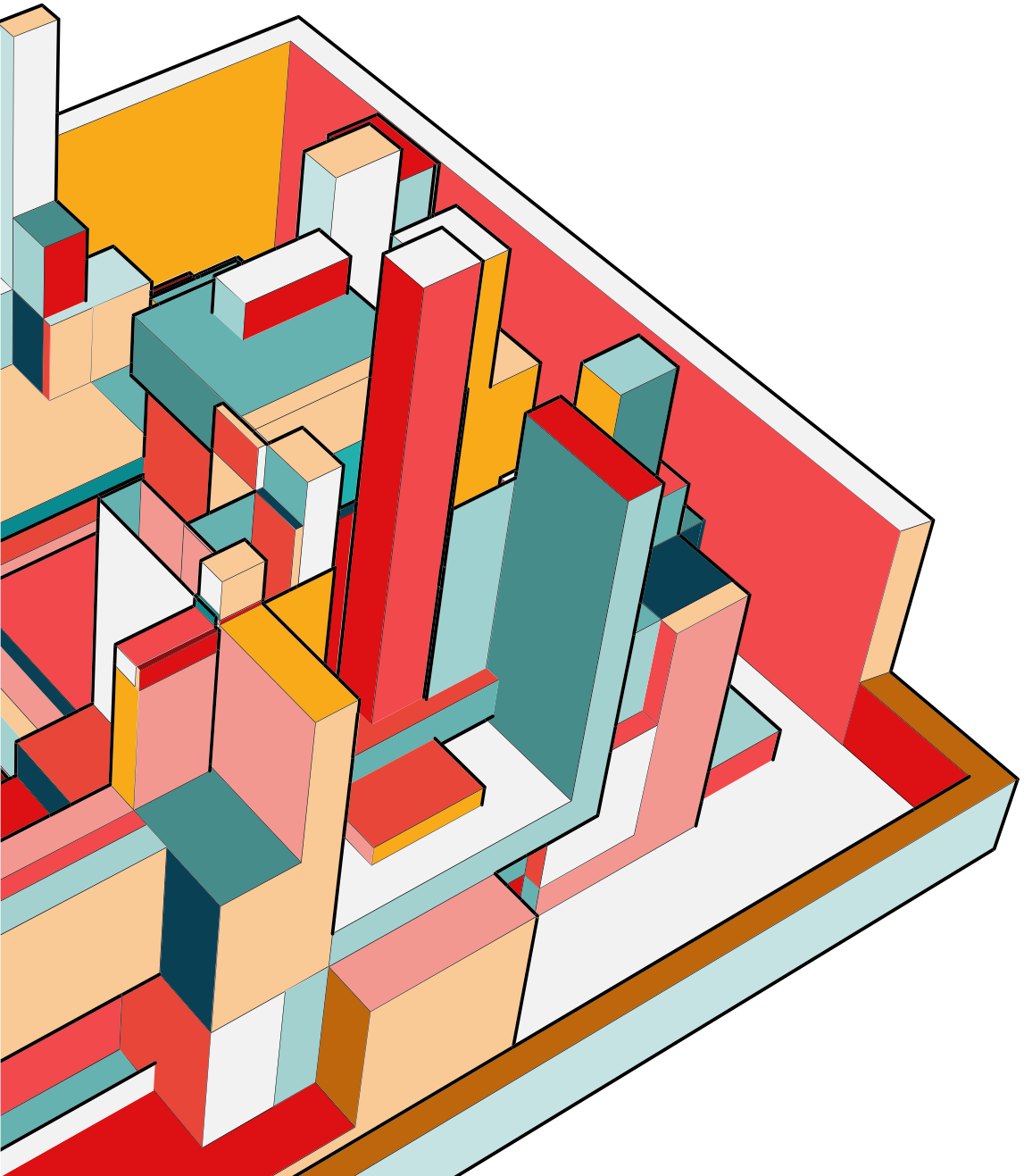
Find Presenters

Reach out to community
Ask after you hear a good one
Pick a focus and search
Look outside

Set a Time and Place

Be consistent
Remember time zones
Make it accessible





EVENTS

Goal: Organize, coordinate, and host OIG community events that encourage interaction of cybersecurity personnel and cross-pollination of security ideas.

EVENTS TASKS

Book Club

Share Ideas

Conference

Bring people together

Challenges

Show off your skills against others

BOOK CLUB EXAMPLES

The Code Book

The Secrets Behind Codebreaking

Sandworm

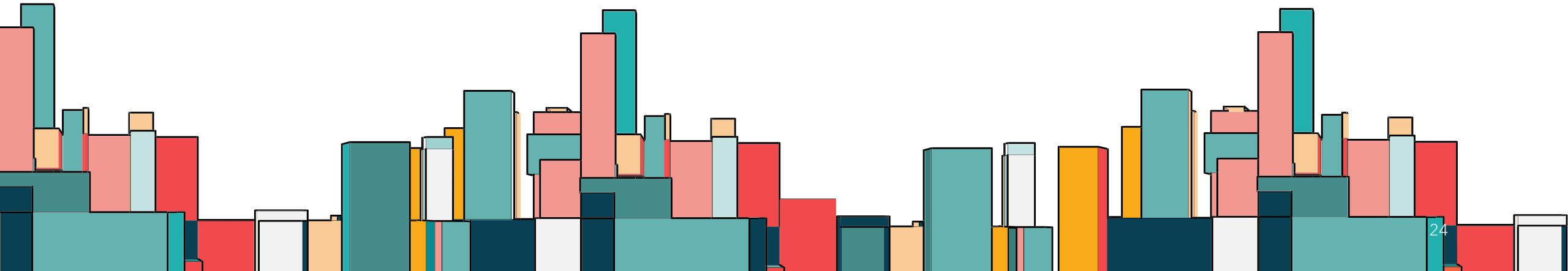
A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers

Dawn of the Code War

America's Battle Against Russia, China, and the Rising Global Cyber Threat

Cult of the Dead Cow

How the Original Hacking Supergroup Might Just Save the World



POSSIBLE FUTURE INITIATIVES

1

Coordinate Policies and Standards

Coordinate

2

Structured learning tracks

3

Cyber Range / Lab Services

SHOW PROGRESS

Start strong to get attention

First Week

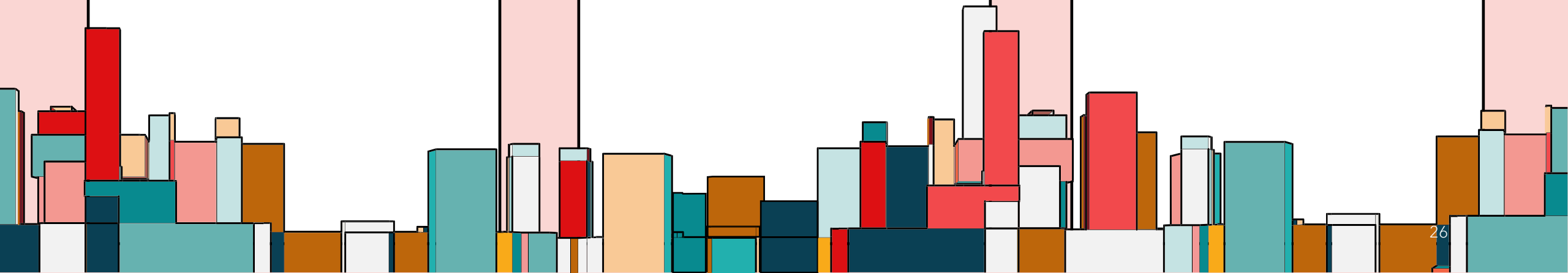
First Group Meeting

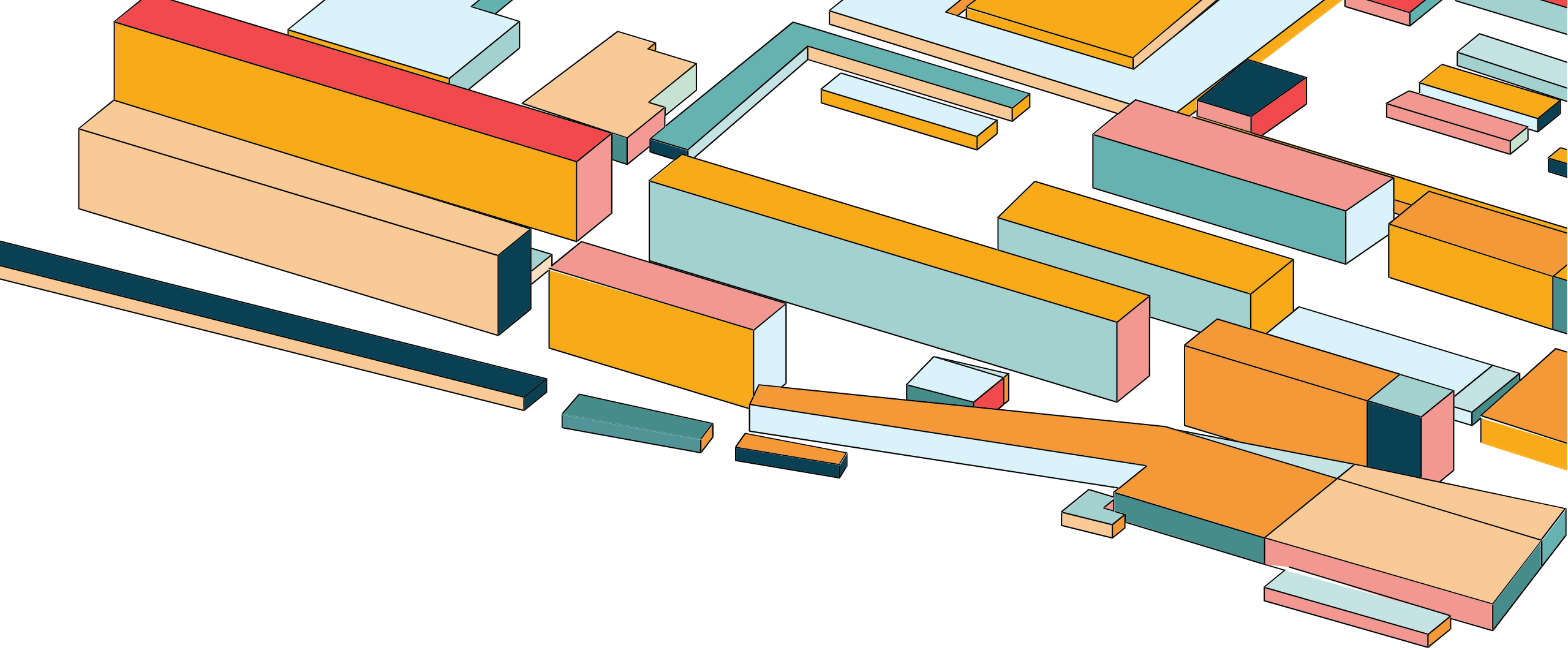
First Month

Newsletter
Big Draw Training

First Quarter

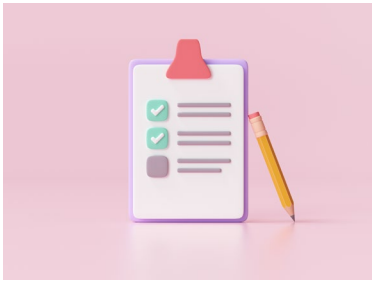
Book Club





BRING PEOPLE TOGETHER

THINK BROADLY



Audit

Investigations

Operations

BIG TEAM MEETING

Discuss Topics

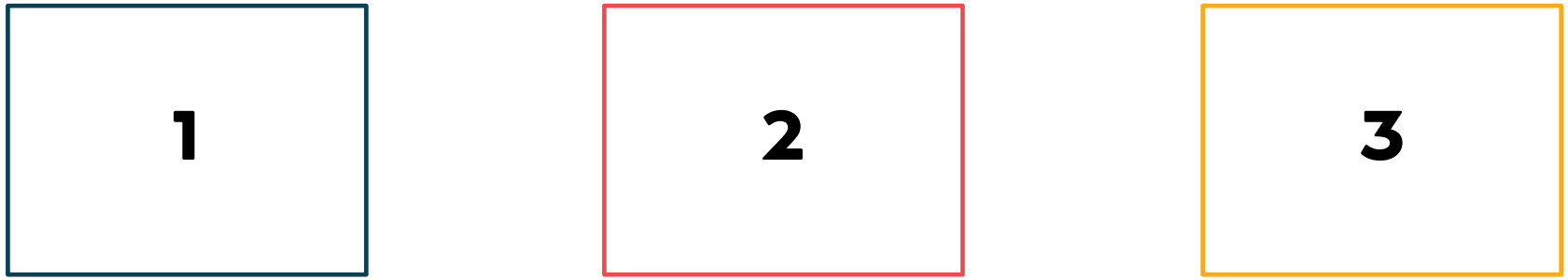
Get People Involved

Pick FutureTasks

POLL #4 – OF THE FOLLOWING THREE, WHAT SECURITY CONTROL FAMILY DO YOU THINK IS MOST IMPORTANT?

1	2	3
Access Control	Configuration Management	Incident Response

POLL #5 DO I REALLY NEED TO ENCRYPT SENSITIVE EMAIL IF IT'S INTERNAL ONLY?



Yes

No

It Depends

POLL #6: WHICH BAD PASSWORD MEETS COMMON SECURITY STANDARDS?

1	2	3
Winter2023	Password1!	qwertyzyuiopasdfghjklz

CHALLENGES

Discussions

Group discussions are sometimes the same voices

Volunteers

Help is hard to find, leads are even harder

Time

Other, other, other duty as assigned

KEEP UP MOMENTUM

Make Participation Easy

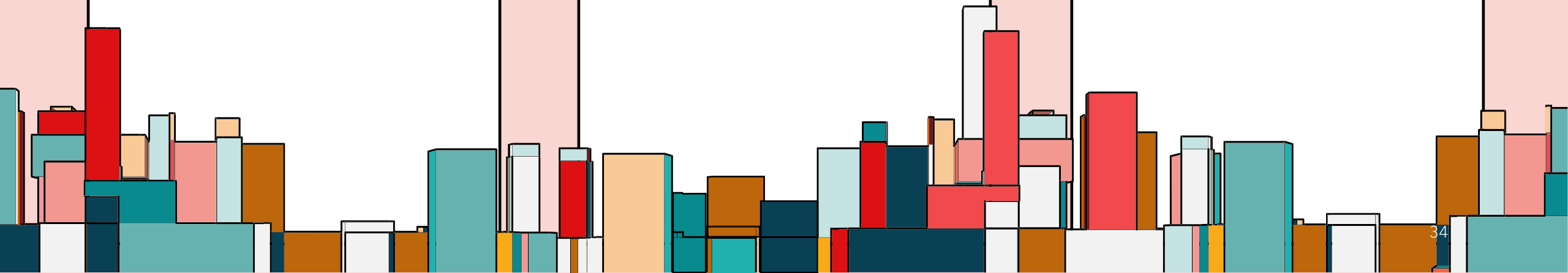
Make joining easy and make effective use of varying skill

Be Consistent

Try to hit the same timeframes every month

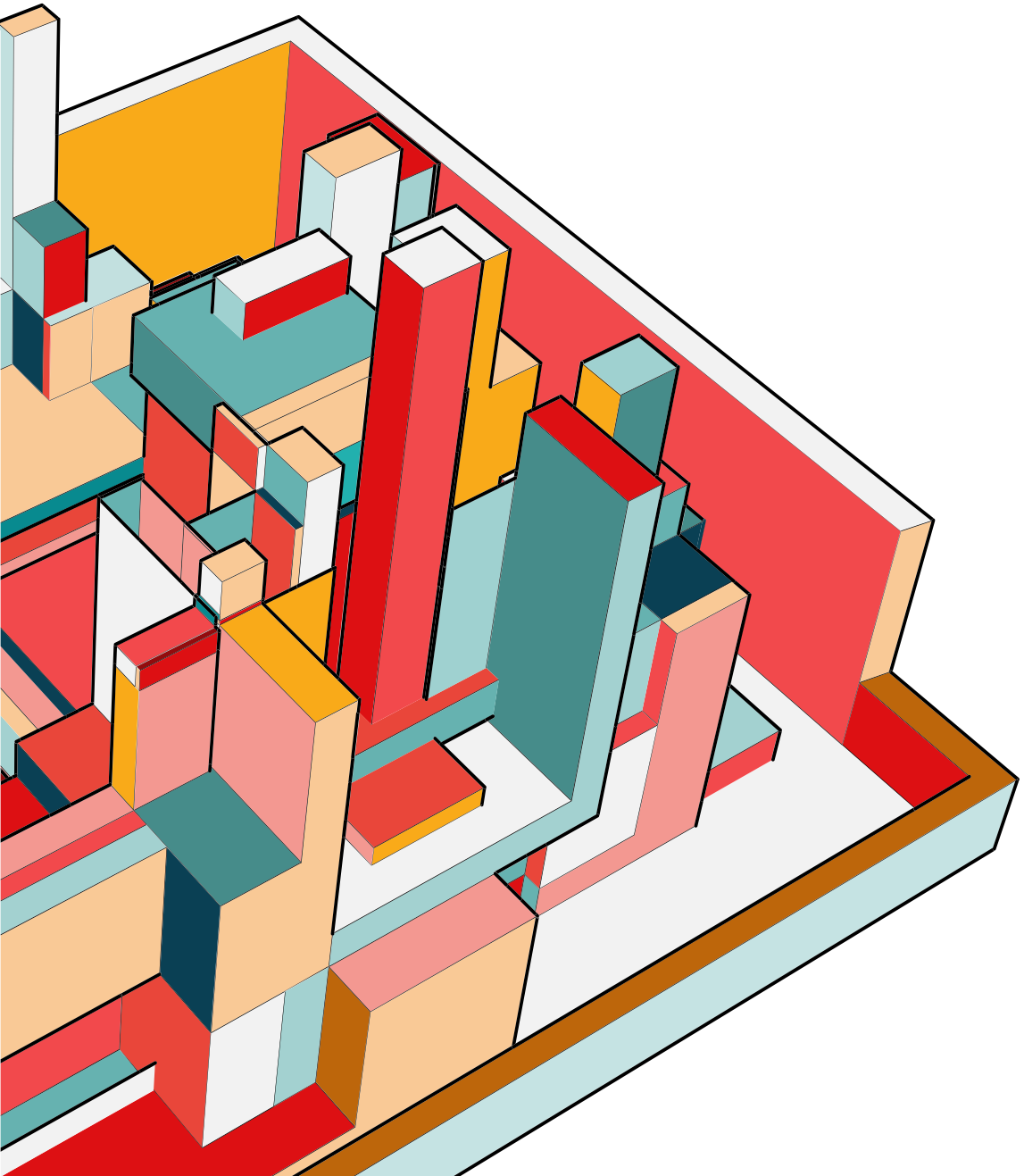
Try New Things

Stay relevant



POLL #7 – DO YOU WANT TO BE INVOLVED IN A CYBERSECURITY WORKING GROUP?

1	2	3
Yep	Maybe	Nope



IN SUMMARY

Vision

Structure

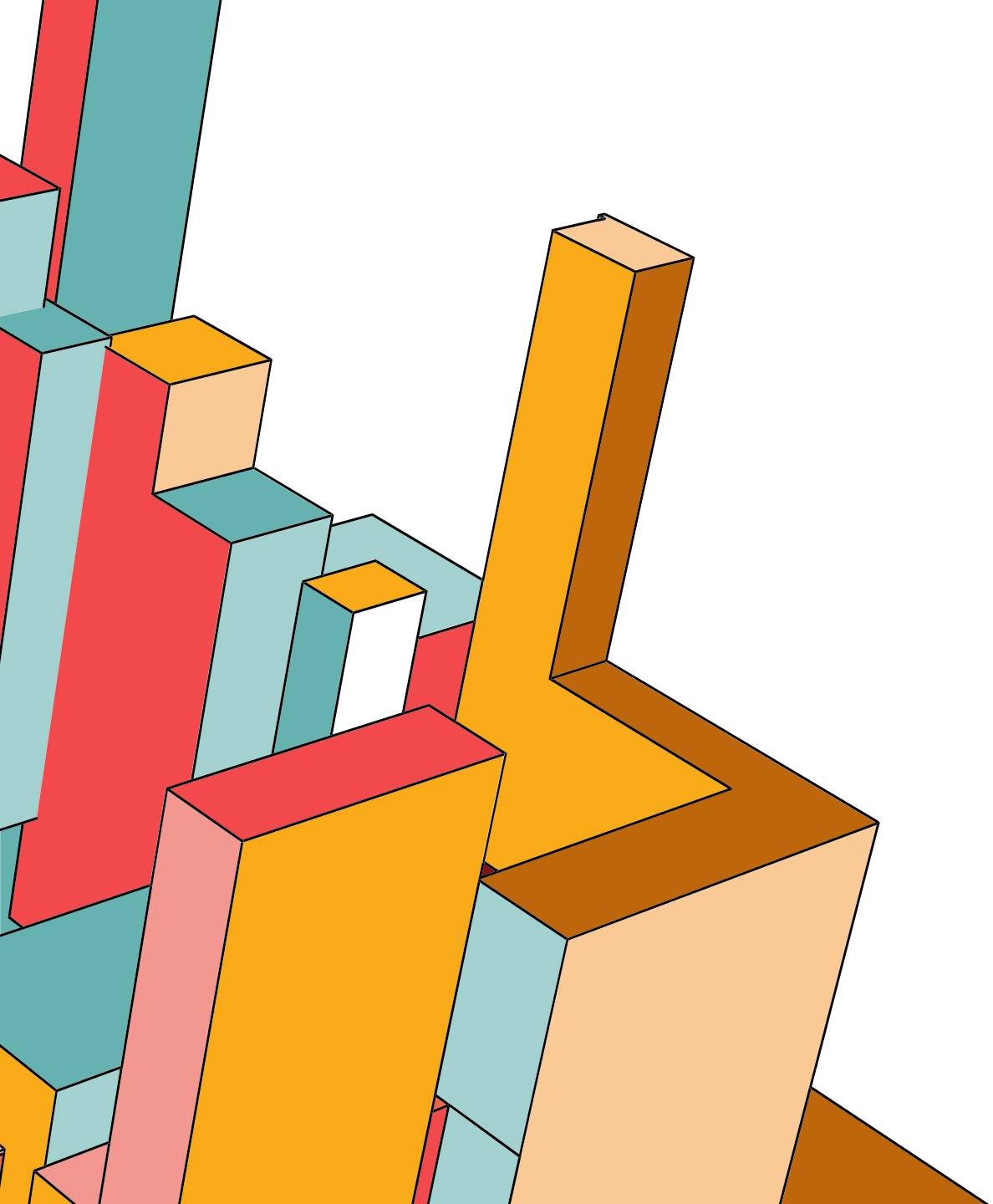
Initiatives

Progress

People

Challenges

Momentum



NOTHING IS PERFECT

THANK YOU

Chuck Mitchell

Director for Cybersecurity

Commerce OIG

cmitchell@oig.doc.gov