NATIONAL
MULTIFAMILY
HOUSING
COUNCIL

Russia’s Ukraine Invasion & Cybersecurity Preparedness

March 11, 2022

Outline

- Introductions
- Road to war
- Threats
- Beyond CRE; critical lifelines & cascading effects
- What organizations should be doing now
    - USG guidance
    - Industry coordination
- Q&A

Outline

- **Introductions**
- Road to war
- Threats
- Beyond CRE; critical lifelines & cascading effects
- What organizations should be doing now
  - USG guidance
  - Industry coordination
- Q&A

Introductions

- Your presenters
- Gate 15
- RE-ISAC
- CCWG
- ISACs, ISAOs, and info sharing

Andy Jabbour

- Co-founder and Managing Director of The Gate 15 Company and founder of Faith-Based Information Sharing & Analysis Organization (FB-ISAO) and the Cannabis ISAO.
- Andy has served as the Managing Director and lead analyst for **RE-ISAC** since 2012.
- He serves on the InfraGardNCR Board and is a member of the International Association of Venue Managers Venue Safety & Security Committee and as faculty for IAVM’s Academy for Venue Safety & Security.
- Andy is an Army veteran with deployments to Kosovo, Iraq, and Afghanistan. He has previously supported the DHS, DOD, NRC, USACE and other USG orgs.

Jennifer Lyn Walker

- **Jennifer** is a cybersecurity professional with over twenty years' experience supporting critical infrastructure and SLTT governments.
- As **Director of Cyber Defense for The Gate 15 Company**, she analyzes, advises, and consults on cyber threats and developing resources and strategies to enhance security and resilience for critical infrastructure and vital lifeline sectors.
- She is a key cybersecurity resource for several ISACs, including WaterISAC, Tribal-ISAC, and RE-ISAC. Jen is experienced in (and passionate for) malware analysis, threat assessments, cyber threat intelligence, compliance, insider threats, cybersecurity awareness, and industrial control system security.

Gate 15

- For-profit, SWaM business, specializing in **analysis**, **preparedness** and **operations**.
- Established 2011, operational since 2013.
- Supports a number of ISACs including RE-ISAC, WaterISAC, Health-ISAC, Auto ISAC, REN-ISAC, Tribal-ISAC, and has spun off two 501c3 non-profit ISAOs focused on faith and cannabis, and works with individual organizations and government entities.

Real Estate ISAC Information Sharing and Analysis Center

Serving the Commercial Facilities Sector

RE-ISAC

- The **Real Estate Information Sharing and Analysis Center (RE-ISAC)** is a public-private partnership between the U.S. Commercial Facilities Sector and federal homeland security officials organized by The Real Estate Roundtable in Feb 2003.
- NMHC, RER and NAREIT are organizational members of RE-ISAC.
- On an operational basis, the RE-ISAC is managed by **The Real Estate Roundtable** and its Homeland Security Task Force.
- RE-ISAC facilitates the **sharing of actionable intelligence, best practices and, other information** to our members.

Commercial Facilities Cyber Working Group (CCWG)

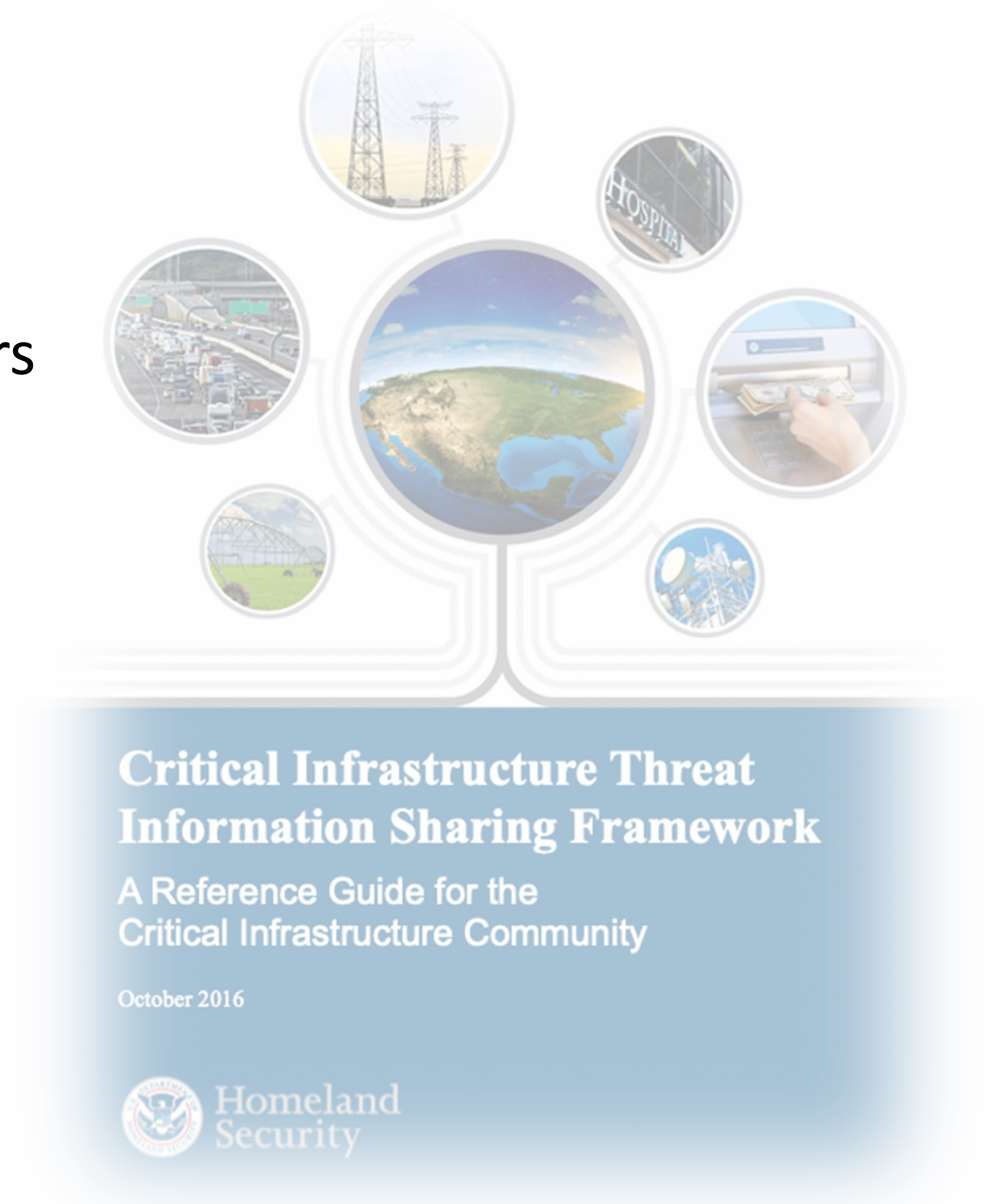
- The FBI’s National Capital Region chapter of InfraGard (InfraGardNCR), in coordination with RE-ISAC, stood up CCWG to support cybersecurity and resilience in the Commercial Facilities Sector.
- CCWG is open to InfraGard members at the intersection of information security and facilities.
- CCWG’s mission is to develop, foster, and facilitate a private-public community of cybersecurity-focused professionals in the Commercial Facilities Sector to facilitate real-time information about risk, governance, emerging threats, best practices.

ISACs, ISAOs & Info Sharing

- Information Sharing and Analysis Centers (ISACs)
- Information Sharing and Analysis Organizations (ISAOs)

'In today's interconnected world, every second can make a difference in either preventing an incident or responding to an event that affects the Nation's critical infrastructure. The ability of federal, state, local, tribal, territorial, and private sector partners to share accurate information quickly is essential to the Nation's security and resilience.'

- https://www.cisa.gov/information-sharing-vital-resource



Critical Infrastructure Threat Information Sharing Framework

A Reference Guide for the
Critical Infrastructure Community

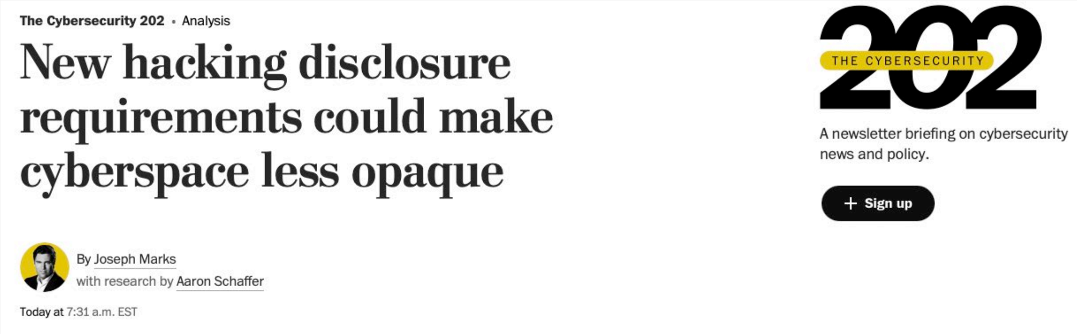
October 2016

Homeland
Security

Cybersecurity Reporting Legislation

- The first is a law that would require companies in critical sectors such as finance, energy and health care to alert the Cybersecurity and Infrastructure Security Agency (CISA) within three days when they're hacked. It's the most expansive cyber reporting requirement government has ever placed on industry. The Senate passed it last night as part of a sweeping $1.5 trillion government funding bill that will soon be signed into law by President Biden.

- The second is a new Securities and Exchange Commission regulation that sets firmer rules for how and when publicly traded companies must disclose significant cyber breaches to the public. The SEC is gathering public feedback now and could finalize the rule within two months.



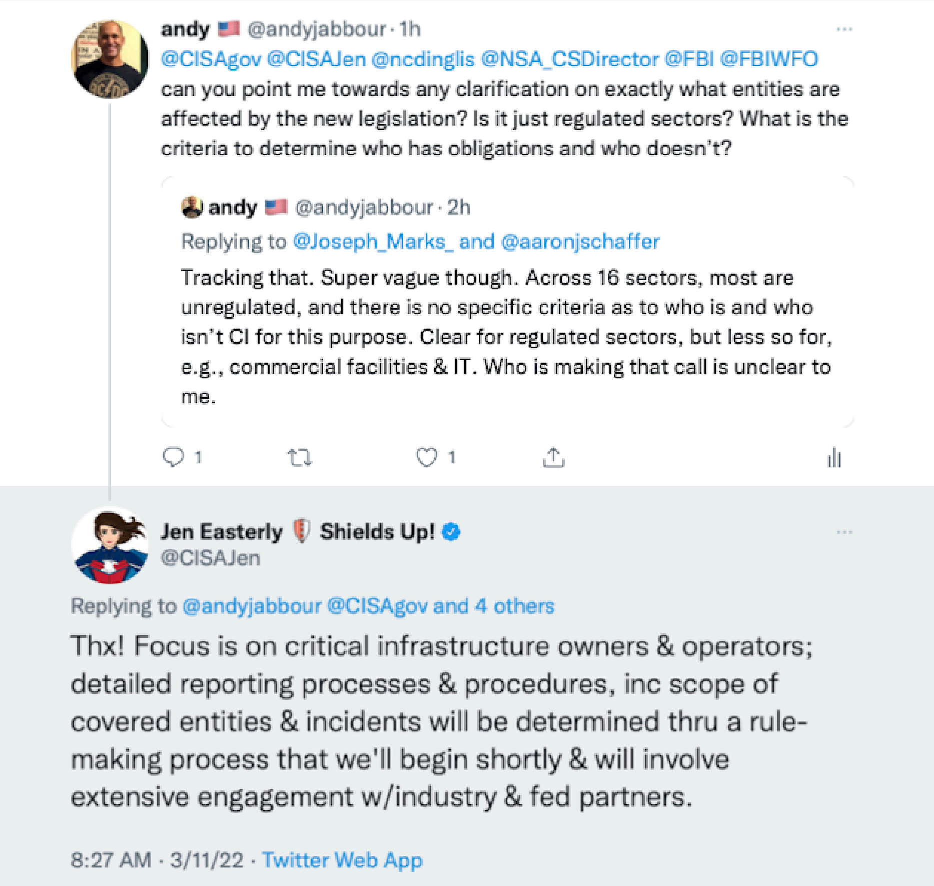
The Cybersecurity 202 · Analysis

New hacking disclosure requirements could make cyberspace less opaque

By Joseph Marks
with research by Aaron Schaffer

Today at 7:31 a.m. EST

A newsletter briefing on cybersecurity news and policy.



andy 🇺🇸 @andyjabbour · 1h
@CISAgov @CISAJen @ncdinglis @NSA_CSDirector @FBI @FBIWFO can you point me towards any clarification on exactly what entities are affected by the new legislation? Is it just regulated sectors? What is the criteria to determine who has obligations and who doesn't?

> andy 🇺🇸 @andyjabbour · 2h
> Replying to @Joseph_Marks_ and @aaronjschaffer
> Tracking that. Super vague though. Across 16 sectors, most are unregulated, and there is no specific criteria as to who is and who isn't CI for this purpose. Clear for regulated sectors, but less so for, e.g., commercial facilities & IT. Who is making that call is unclear to me.

Jen Easterly 🛡️ Shields Up! ✓
@CISAJen
Replying to @andyjabbour @CISAgov and 4 others

Thx! Focus is on critical infrastructure owners & operators; detailed reporting processes & procedures, inc scope of covered entities & incidents will be determined thru a rule-making process that we'll begin shortly & will involve extensive engagement w/industry & fed partners.

8:27 AM · 3/11/22 · Twitter Web App

Outline

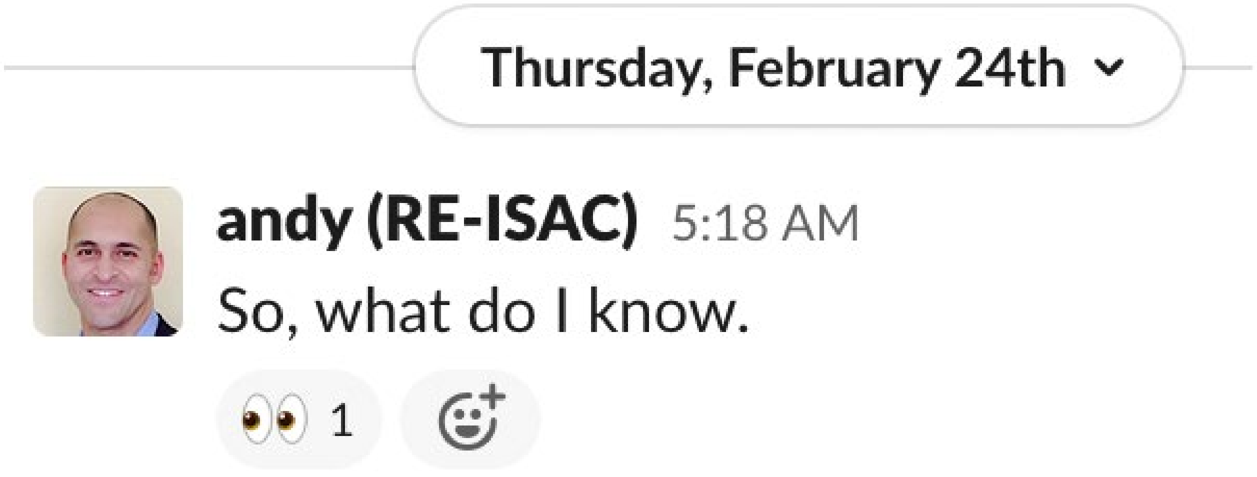
- Introductions
- **Road to war**
- Threats
- Beyond CRE; critical lifelines & cascading effects
- What organizations should be doing now
  - USG guidance
  - Industry coordination
- Q&A

Road to war

- **10 Nov**: US reports unusual movement of Russian troops near the borders of Ukraine.
- **28 Nov**: Ukraine reported a build up of 92,000 Russian troops.
- **07 Dec**: President Biden warned Putin of “strong economic and other measures” if Russia attacks Ukraine.
- **17 Dec**: Putin proposed limits on NATO's activities in eastern Europe, such as a prohibition on Ukraine ever joining NATO, which are rejected.
- **17 Jan**: Russian troops began arriving in Russia's ally Belarus for military exercises.
- **19 Jan**: US provides Ukraine $200 million in security aid.
- **24 Jan**: NATO put troops on standby.
- **25 Jan**: Russian exercises take place in Russia near Ukraine, and Crimea.

Road to war

- **10 Feb**: Russia and Belarus began 10 days
- **17 Feb**: Fighting escalated in separatist reg
- **21 Feb**: President Putin announced that Ru regions in eastern Ukraine.
- **22 Feb**: First round of economic sanctions
- **24 Feb**: Shortly before 6:00 am Moscow Ti launch a “special military operation” in eas plans to occupy Ukrainian territory and tha self-determination. Putin also stated that F of Ukraine. Within minutes of Putin's anno



Thursday, February 24th ⌄

andy (RE-ISAC) 5:18 AM

So, what do I know.

👀 1

Andy, admitting he knows nothing, in a Slack message to a peer, regarding previous confidence that Russia would not invade Ukraine. Andy, in a message on 19 Feb, ‘Despite the headlines, I still see him having more to lose... I may wake up w a lot of egg on my face though...’ Egg is still sliding down Andy’s back at this time.

Outline

- Introductions
- Road to war
- **Threats**
- Beyond CRE; critical lifelines & cascading effects
- What organizations should be doing now
  - USG guidance
  - Industry coordination
- Q&A

Threats: Physical

- Indirect threats associated with mass gatherings
- Vandalism
- Potential targeting of tenants
- Russian fomenting of inter-personal tensions
    - Anti-Semitism; Russia and the manipulation of faith
    - Political / Conspiracy theories
    - Racial

Threats: Misinformation

"Beyond its invasion of Ukraine, Moscow presents a serious cyber threat, a key space competitor, and one of the most serious foreign influence threats to the United States. Using its intelligence services, proxies, and wide-ranging influence tools, ***the Russian government seeks to not only pursue its own interests but also to divide Western alliances, undermine U.S. global standing, amplify discord inside the United States, and influence U.S. voters and decision making****."*

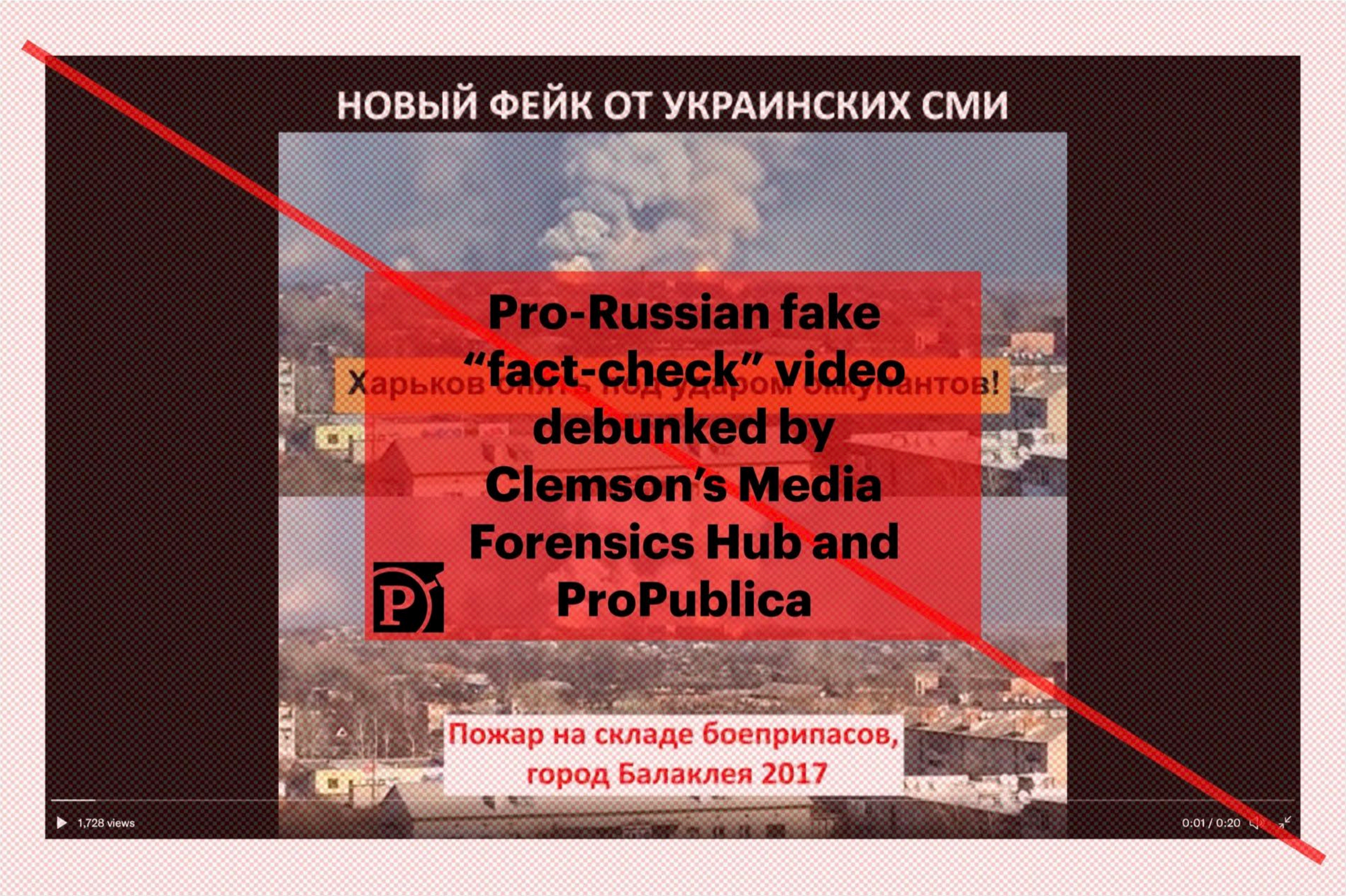
- Avril Haines, Director of National Intelligence Congressional Testimony, Annual Threat Assessment of the U.S. Intelligence Community, 08 March 2022

Threats: Misinformation

- State media reports false information; reporting events the way they would like them to seed their information operations:
  - Breakaway regions
  - Ukrainian threats
  - US bioweapons manufacturing

- On social media, there are posts “debunking” alleged Ukrainian disinformation. These debunking items themselves are fake and then get reported. Causes confusion; manipulates local population and garners support.

- Chinese media is increasingly reporting Russian misinfo.


НОВЫЙ ФЕЙК ОТ УКРАИНСКИХ СМИ
Харьков опять под ударом оккупантов!
Пожар на складе боеприпасов, город Балаклея 2017
Pro-Russian fake “fact-check” video debunked by Clemson’s Media Forensics Hub and ProPublica
1,728 views
0:01 / 0:20

Stills from a Russian-language video that falsely claims to fact-check Ukrainian disinformation. There’s no evidence the video was created by Ukrainian media or circulated anywhere, but the label at the top says the video is a “New Fake from Ukrainian media.” The central caption inaccurately labels the footage as “Kharkiv is again under attack by the occupants!” falsely attributing the claim to Ukrainian media. The lower caption correctly identifies the event as “Fire at the ammunition depot, the city of Balakliya, 2017.” Screenshot taken by ProPublica

Threats: Cyber

- **13 Jan**: "WhisperGate" wiper activity targets Ukrainian organizations, including Ukrainian government agencies.
- **23 Feb**: Distributed denial-of-service (DDoS) attack on Ukrainian organizations, including Ukrainian government agencies. HermeticWiper malware used to attack Ukrainian organizations.
- **25 Feb**: Conti ransomware actors published a series of statements regarding their stance in the context of the Russia-Ukraine conflict.
- Ongoing reports of independent attacks against Russia – from cameras to government agencies and attacks aimed at Ukrainian citizens

Threats: Cyber

- **The number one concern is a direct ransomware attack.**
- **The secondary concern is ransomware attack on others with cascading effects** (suppliers, lifelines [more to follow]).
- Other concerns include third party attacks, Zero Day attacks, DDoS, wiper attacks, hacktivism, credential harvesting, and other common attacks.

Outline

- Introductions
- Road to war
- Threats
- **Beyond CRE; critical lifelines & cascading effects**
- What organizations should be doing now
  - USG guidance
  - Industry coordination
- Q&A

Beyond CRE; critical lifelines & cascading effects

- Potential attacks against critical lifelines
  - Water
  - Power
  - Comms/IT
  - Vital Services (Transportation, Health, Financial Services, etc.)

- Is your organization prepared for potential disruptions?

Outline

- Introductions
- Road to war
- Threats
- Beyond CRE; critical lifelines & cascading effects
- **What organizations should be doing now**
  - **USG guidance**
  - **Industry coordination**
- Q&A

What organizations should be doing now

USG Guidance

- While there are no specific or credible cyber threats to the U.S. homeland at this time, Russia’s unprovoked attack on Ukraine, which has involved cyber-attacks on Ukrainian government and critical infrastructure organizations, may impact organizations both within and beyond the region.
- Every organization—large and small—must be prepared to respond to disruptive cyber activity.

What organizations should be doing now

USG Guidance

- Reduce the likelihood of a damaging cyber intrusion.
- Take steps to quickly detect a potential intrusion.
- Ensure that the organization is prepared to respond if an intrusion occurs.
- Maximize the organization's resilience to a destructive cyber incident.

What organizations should be doing now

USG Guidance

- **Empower** Chief Information Security Officers (CISO).
- **Lower Reporting Thresholds**.
- Participate in a **Test of Response Plans.**
- **Focus on Continuity.**
- Plan for the Worst.

What organizations should be doing now

USG Guidance

- **Prepare for a ransomware attack**.
- There is abundant government and industry guidance on how to prepare for a ransomware attack.

What organizations should be doing now

USG Guidance

- Review recent cybersecurity advisories.
- **Know your networks;** especially if you have even a tangential relationship with Russia and surrounding countries.
- Know your **Cyber Incident Response plan.** If you don't have one, you should.
- Report mis, dis, mal information, a tried-and-true tactic of the Russian government, including on your social media.
- In the event of a compromise, call the FBI.

What organizations should be doing now

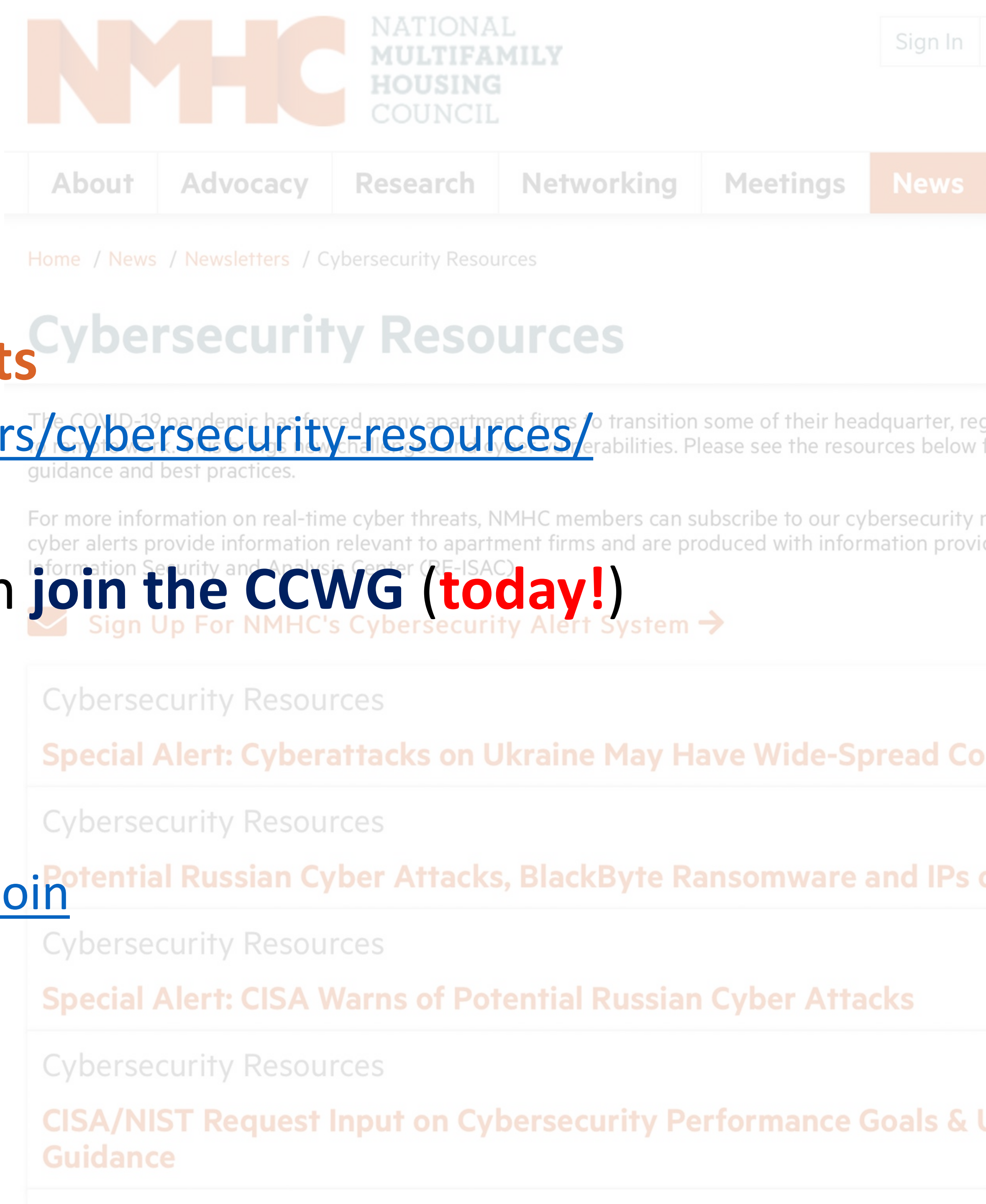
Industry Coordination

- Sign up for **NMHC Cybersecurity Alerts**
  - https://www.nmhc.org/news/newsletters/cybersecurity-resources/
- Have someone from your organization **join the CCWG** (**today!**)
  - https://cf.epicplatform.com
- Consider joining **RE-ISAC**
  - https://www.reisac.org/about-the-isac/join

Real Estate ISAC Information Sharing and Analysis Center

Serving the Commercial Facilities Sector

CCWG COMMERCIAL FACILITIES CYBER WORKING GROUP


NMHC NATIONAL MULTIFAMILY HOUSING COUNCIL
Sign In
About
Advocacy
Research
Networking
Meetings
News
Home / News / Newsletters / Cybersecurity Resources

Cybersecurity Resources

The COVID-19 pandemic has forced many apartment firms to transition some of their headquarter, reg to remote work. This brings new challenges and cyber vulnerabilities. Please see the resources below f guidance and best practices.

For more information on real-time cyber threats, NMHC members can subscribe to our cybersecurity r cyber alerts provide information relevant to apartment firms and are produced with information provi Information Security and Analysis Center (RE-ISAC).

Sign Up For NMHC's Cybersecurity Alert System →

Cybersecurity Resources

Special Alert: Cyberattacks on Ukraine May Have Wide-Spread Co

Cybersecurity Resources

Potential Russian Cyber Attacks, BlackByte Ransomware and IPs o

Cybersecurity Resources

Special Alert: CISA Warns of Potential Russian Cyber Attacks

Cybersecurity Resources

CISA/NIST Request Input on Cybersecurity Performance Goals & U Guidance

Outline

- Introductions
- Road to war
- Threats
- Beyond CRE; critical lifelines & cascading effects
- What organizations should be doing now
  - USG guidance
  - Industry coordination
- **Q&A**

Thank you

Julianne B. Goodfellow
Vice President, Government Affairs, NMHC
jgoodfellow@nmhc.org

Andy Jabbour
Co-founder and Managing Director, The Gate 15 Company
andy@reisac.org or andy@gate15.global

Jennifer Lyn Walker
Director of Cyber Defense, The Gate 15 Company
Jennifer@gate15.global