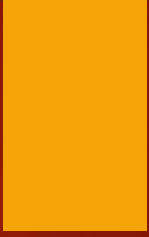


U.S. National Cyber Strategy



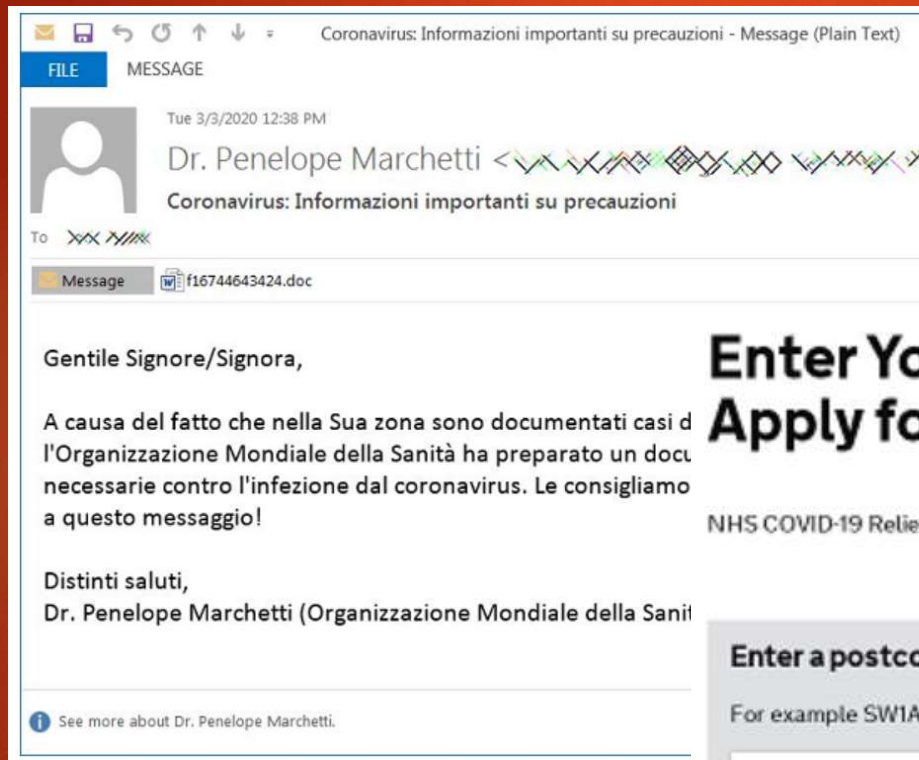
U.S. EMBASSY ROME, ITALY

John T. Conway

Information Management Officer

U.S. Department of Homeland Security

2



URGENT: UKGOV has issued a payment of 458 GBP to all residents as part of its promise to battle COVID 19. TAP here <https://uk-covid-19.webredirect.org/> to apply

Enter Your Post Code To Apply for COVID-19 Relieve

NHS COVID-19 Relieve system.

Enter a postcode

For example SW1A 2AA

Find

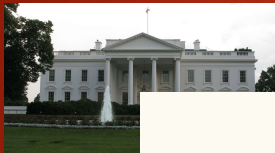
U.S. National Cyber Strategy

3

- ▶ What is the U.S. strategy for cybersecurity?
- ▶ How does the entire U.S. federal government implement the strategy?
- ▶ How does the U.S. Embassy implement the cybersecurity strategy in Italy?

U.S. National Cyber Strategy

4



With the release of this National Cyber Strategy, the United States now has its first fully articulated cyber strategy in 15 years. This strategy explains how my Administration will:

- Defend the homeland by protecting networks, systems, functions, and data;
- Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;
- Preserve peace and security by strengthening the ability of the United States – in concert with allies and partners – to deter and, if necessary, punish those who use cyber tools for malicious purposes; and
- Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.

U.S. National Cyber Strategy

5

Defend the Homeland

OBJECTIVE: Manage cybersecurity risks to increase the security and resilience of the Nation's information and information systems.

U.S. National Cyber Strategy

6

Promote American Prosperity

OBJECTIVE: Preserve U.S. influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth innovation, and efficiency.

U.S. National Cyber Strategy

7

Preserve Peace through Strength

OBJECTIVE: Identify, counter, disrupt, degrade and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving U.S. overmatch and and through cyberspace.

U.S. National Cyber Strategy

8

Advance American Influence

OBJECTIVE: Preserve the long-term openness, interoperability, security, and reliability of the Internet, which supports and is enforced by U.S. interests.



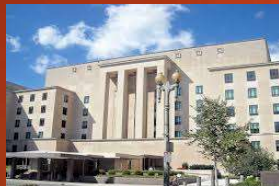
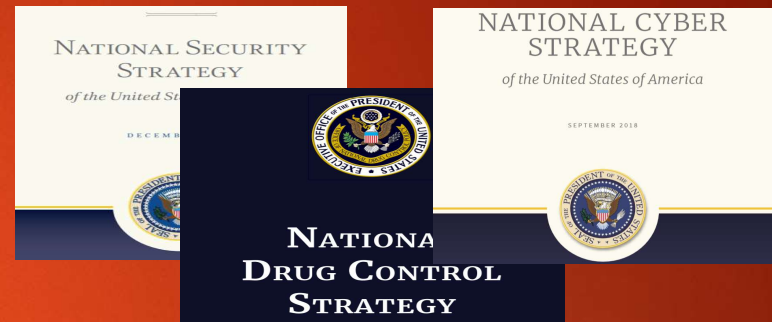
Security and Economy

Security of the Economy

Executive Branch



Implements and Enforces Laws



Leads Foreign Policy

Performance Goal 1.4.1

By 2022, significantly increase international cooperation to secure an open, interoperable, reliable, and stable cyberspace and strengthen the capacity of the United States and partner nations to detect, deter, rapidly mitigate, and respond to international cyber threats and incidents.



Conducts Diplomatic Relations



Italy and The Republic of San Marino

11



Integrated Country Strategy

Italy and
The Republic of San Marino

Mission Goal 1: Italy Counters Threats to the United States and the International Order, and Together Italy and the United States Advance Civilian Security around the World.

Mission Objective 1.1: The United States and Italy continue robust foreign policy, defense, and basing cooperation to address threats and advance security around the world.

Mission Objective 1.2: Italy strengthens its capacity to counter terrorism, corruption, cyber threats, and transnational criminal activity, and continues to collaborate with the United States to protect America's borders and infrastructure.

National Institute of Standards and Technology (NIST)

12

Cybersecurity Framework (Federal Networks & Public Infrastructure)

NIST
CYBERSECURITY FRAMEWORK [Helping organizations]

- Framework +
- New to Framework +
- Perspectives +
- Success Stories +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations +
- Related Efforts (Roadmap) +
- Informative References +
- Resources +
- Newsroom +
- Related Programs +

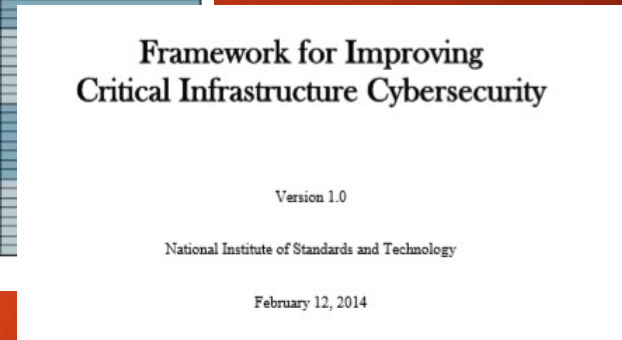
Framework Version 1.1
The Cybersecurity Framework is ready to download.
[Learn More](#)

New to Framework
This voluntary Framework consists of standards, guidelines and best practices to manage cybersecurity risk.
[Learn More](#)

Online Learning
Intro material for new Framework users to implementation guidance for more advanced Framework users.
[Learn More](#)

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Figure 1: Framework Core Structure



Documentation

Approved/Tested Devices

U.S. National Cyber Strategy

Outreach & Cooperation

- Economics Office
 - Political Officers
 - Federal Bureau of Investigation
 - U.S. Secret Service
 - Etc.
-
- November 25th, 2019, European Electronic Crimes Task Force Meeting

U.S. National Cyber Strategy

Attribution - State-sponsored Activities

Chinese cyber actors associated with the Chinese Ministry of State Security



Cyber actors of the North Korean government

Russian State-Sponsored
Cyber Actors

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor
<https://www.cisa.gov/cisa/cybersecurity>

U.S. National Cyber Strategy

15

Trusted Sources vs. Untrusted Sources

Authoritarian governments lack an independent judiciary and rule of law that prevents misuse of data.



Changes in Functionality:

- Software updates
- Patches

Back doors to
“Customer data” and
“IP Movements”

U.S. National Cyber Strategy

16

- ▶ What is the U.S. strategy for cybersecurity?
- ▶ How does the entire U.S. federal government incorporate the strategy?
- ▶ How does the U.S. Embassy implement the cybersecurity strategy in Italy?

U.S. Embassy Rome

17

Follow us!



<https://twitter.com/AmbasciataUSA>



<https://www.facebook.com/AmbasciataUSA/>



<https://www.instagram.com/AmbasciataUSA>