FDA U.S. FOOD & DRUG ADMINISTRATION

Cybersecurity Modernization Action Plan

U.S. Food and Drug Administration

Office of Information Security
Office of Digital Transformation

November 2022

Lincoln Sea
Beaufort Sea
Queen Elizabeth
GREENLAND (Denmark)
Greenland Sea
Norwegian Sea
Baffin Bay
Davis Strait
Denmark Strait
Nunavut Territory
ALASKA (U.S.A.)
Anchorage
ICELAND
Reykjavik
NORWAY
Oslo
C A N A D A
Gulf of Alaska
Rocky Mountains
Hudson Bay
Labrador Sea
Quebec
Edmonton
Calgary
Regina
Winnipeg
Vancouver
Seattle
Portland
Quebec
Ottawa
Montreal
Toronto
Detroit
Boston
Chicago
New York
Philadelphia
Washington
Baltimore
Salt Lake City
Denver
Kansas City
St. Louis
Sacramento
San Francisco
UNITED STATES OF AMERICA
Los Angeles
San Diego
Mexicali
El Paso
Dallas
Memphis
Atlanta
Houston
New Orleans
San Antonio
Monterrey
Gulf of Mexico
Miami
NORTH ATLANTIC OCEAN
BAHAMAS
Havana
CUBA
MEXICO
Tampico
Guadalajara
Merida
Cancun
Mexico
Acapulco
DOMINICAN REP.
HAITI
Port-au-Prince
Santo Domingo
ST KITTS AND NEVIS
ANTIGUA AND BARBUDA
DOMINICA
BELIZE
JAMAICA
HONDURAS
GUATEMALA
EL SALVADOR
NICARAGUA
COSTA RICA
Caribbean Sea
ST LUCIA
GRENADA
BARBADOS
ST VINCENT AND THE GRENADINES
TRINIDAD AND TOBAGO
Maracaibo
Merida
Caracas
PANAMA
VENEZUELA
Georgetown
Paramaribo
GUYANA
FRENCH GUYANA (France)
SURINAME
Medellin
Bogota
Cali
COLOMBIA
Boa Vista
NORTH PACIFIC OCEAN
Quito
ECUADOR
Guayaquil
Iquitos
Manaus
Belem
Sao Luis
Fortaleza
Teresina
Natal
Recife
Amazon Basin
Porto Velho
PERU
Trujillo
Lima
Cuzco
BRAZIL
Aracaju
Salvador
Cuiaba
Brasilia
La Paz
BOLIVIA
Sucre
Arica
Iquique
Antofagasta
Belo Horizonte
Vitoria
PARAGUAY
Rio de Janeiro
Sao Paulo
Asuncion
Curitiba
Florianopolis
SOUTH ATLANTIC OCEAN
Cordoba
Santa Fe
Porto Alegre
URUGUAY
Rosario
Valparaiso
Santiago
Buenos Aires
Montevideo
La Plata
Concepcion
CHILE
Bahia Blanca
ARGENTINA
SOUTH PACIFIC OCEAN
Patagonia
Strait of Magellan
Falkland Islands (U.K.)
Punta Arenas
Cape Horn
Edinburgh
North Sea
UNITED KINGDOM
DENMARK
Copenhagen
Belfast
Dublin
IRELAND
Manchester
Cardiff
London
Hamburg
Amsterdam
NETH.
BEL.
GERMANY
Paris
FRANCE
Lyon
Marseille
Monaco
AND.
Porto
PORTUGAL
Lisbon
Madrid
SPAIN
Barcelona
Sevilla
Algiers
Oran
Constantine
Rabat
Fes
Casablanca
Marrakesh
TUNISIA
MOROCCO
ALGERIA
WESTERN SAHARA
Sahara
MAURITANIA
MALI
NIGER
CAPE VERDE
Nouakchott
Dakar
SENEGAL
Praia
GAMBIA
Bamako
BURKINA
Niamey
GUINEA-BISSAU
GUINEA
Ouagadougou
NIGERIA
Conakry
COTE DIVOIRE
GHANA
BENIN
Abuja
Freetown
SIERRA LEONE
Monrovia
Yamoussoukro
Accra
Lagos
LIBERIA
Abidjan
TOGO
EQUAT. GUINEA
SAO TOME AND PRINCIPE
GABON
TROPIC OF CANCER
EQUATOR
TROPIC OF CAPRICORN
Amundsen Sea
Bellingshausen Sea
Weddell Sea
A N T A R

EXECUTIVE SUMMARY

Cybersecurity is among the top priorities of the U.S. Food and Drug Administration (FDA), and we take our responsibility seriously to protect industry and public health information in today's environment of increased cybersecurity threats. The FDA Office of Digital Transformation (ODT) recognizes the risks associated with operating a global information technology enterprise in support of our public health mission. ODT has developed this Cybersecurity Modernization Action Plan (CMAP) to strengthen our ability to protect sensitive information, modernize cybersecurity capabilities, and improve situational awareness to decrease overall security risks to the Agency.

As the nation's regulatory organization for public health, the FDA plays a critical role in advancing medical innovation based on sound science, data, and patient-centered approaches. Our global public health mission requires using complex and real-time data to identify meaningful patterns, gain new insights, and inform regulatory decision-making. The rapid pace of healthcare innovation coupled with exponential data growth is driving the Agency's modernization efforts to improve regulatory operations while at the same time establishing new pathways for exchanging data with industry. This modernization includes bold new technological innovation approaches to leverage the power of real-world data and evidence to accelerate regulatory decision-making and new product development. The FDA is also working to harness the power of Artificial Intelligence (AI) to establish new cloud-based data lakes. These data lakes will provide an elastic computational infrastructure, high-performance computing, and enhanced analytics capabilities for structured and unstructured data. Among these advances are the modernization of cybersecurity capabilities and architectures that proactively and comprehensively identify and mitigate risk. The use of innovative cybersecurity approaches to facilitate secure data sharing and enable discovery is becoming increasingly necessary due to exponential increases in the complexity of data in this new environment of misinformation, disinformation, and sophistication of cyber threat actors.

As outlined in the *National Counterintelligence Strategy of the United States*, threat actors have increasingly sophisticated intelligence capabilities at their disposal, which they employ in new and evolving ways to target U.S. government entities, global allies, academia, and the private sector. The global availability of technologies with intelligence applications and the unauthorized disclosures of U.S. cyber tools have enabled a broader range of actors to obtain highly technical capabilities previously possessed by well-financed nation-state intelligence services. At the same time, the proliferation of technological advances in all sectors has led to increasing vulnerabilities available for exploitation. The FDA will continue to focus resources to prevent, protect, detect, respond, and recover from these evolving risks by adopting advanced and innovative tools and technologies while continuing to incorporate counterintelligence and insider risk principles into our intelligence-driven approach.

FDA CYBERSECURITY MISSION AND STRATEGIC PRIORITIES

The mission of the FDA's Cybersecurity, Counterintelligence, and Insider Threat Program is to provide real-time cybersecurity capabilities and risk management methodologies to protect sensitive data and information systems in support of the FDA's public health mission. Our vision is to provide a best-in-class, intelligence-driven cybersecurity program that directly supports the FDA's mission to protect and promote U.S. public health. As FDA's cybersecurity program remains progressively focused on enterprise-wide cyber defenses, our objectives will be achieved through and guided by the continued advancement of our six Strategic Priorities, as outlined in FDA's *Cybersecurity Strategic Plan 2022 - 2025:*

Strategic Priorities
Priority 1: Data and Information Protection
Priority 2: Cybersecurity, Innovation, and Technology
Priority 3: Cyber, Threat, and Vulnerability Management
Priority 4: Cybersecurity Risk and Compliance
Priority 5: Customer Engagement and Cybersecurity Workforce Development
Priority 6: Counterintelligence and Insider Threat

The Office of Digital Transformation (ODT) will upgrade, enhance, and modernize our critical cyber defenses to address the evolving threat landscape where risks to our critical assets, industry, and sensitive data remain moderately high. For example, compared to pre-pandemic, FDA has experienced a 457% increase in reconnaissance activities, denial of service, attempted exploitation, and other cyber incidents against the IT infrastructure.

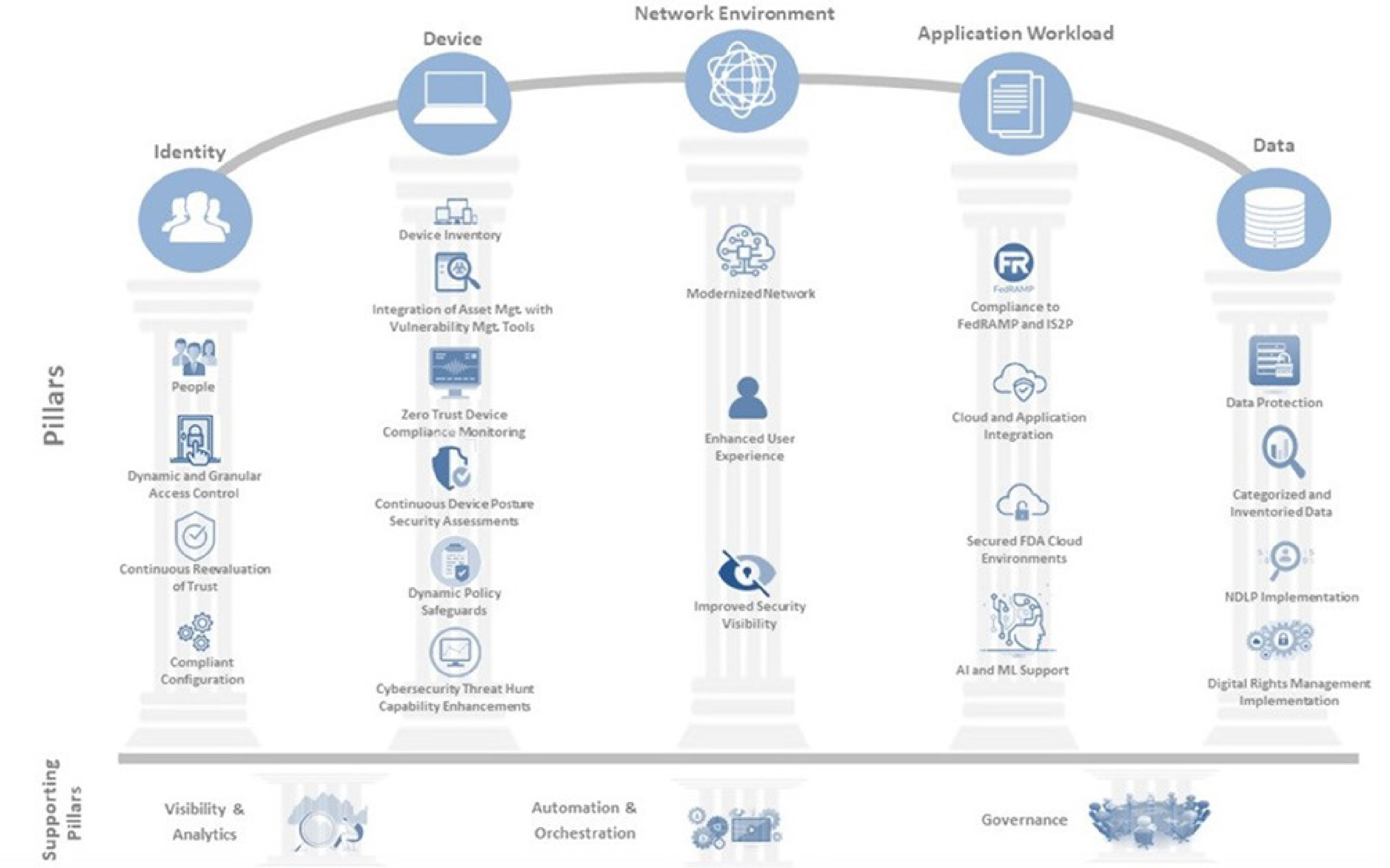
In addition, Presidential Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, issued May 2021, directs agencies to modernize their cybersecurity capabilities. FDA is enhancing our cybersecurity protections by implementing Zero Trust, secure cloud computing, multi-factor authentication, encryption, threat detection, vulnerability management, and other cyber defense capabilities. The CMAP, Presidential Executive Order 14028 *Improving the Nation's Cybersecurity*, Office of Management and Budget OMB M-22-09 *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, and other cybersecurity initiatives align with the FDA's Cybersecurity Strategic Plan 2022-2025. These efforts also support the FDA's Technology Modernization Action Plan, Data Modernization Action Plan, and Enterprise Modernization Action Plan.

ODT has developed the FDA Zero Trust Cybersecurity Network Defense Implementation Plan that will serve as a roadmap to effectively modernize and transition to a Zero Trust model. The plan outlines an incremental approach to prioritize, initiate, execute, mature, and monitor progress as the Agency modernizes and deploys new digital services and facilitates increased ecosystem interactions and data sharing across its global regulatory environment. Implementing a Zero Trust cybersecurity model will support the Agency in building a modern security architecture to expedite digital transformation.

ZERO TRUST CYBERSECURITY NETWORK DEFENSE IMPLEMENTATION PLAN: SUMMARY

The FDA Zero Trust Cybersecurity Network Defense Implementation Plan builds on the fundamental cybersecurity concepts and technologies to attain an optimal maturity level. The plan includes upgrading, modernizing, and enhancing our security and cyber defenses to address evolving threats, vulnerabilities, and risks to the FDA's IT infrastructure and sensitive data.

To execute our plan, we developed the Zero Trust Cybersecurity Network Defense Implementation Initiative to align our current and future cybersecurity capabilities to establish a modern security architecture and facilitate enterprise-wide adoption of a comprehensive Zero Trust framework. The initiative includes three key areas: Initiative Coordination and Oversight, Primary Pillars, and Support Pillars. The FDA will apply subject matter expertise, coordination, and oversight resources to each of these activities to successfully implement our Zero Trust objectives.


Identity
Device
Network Environment
Application Workload
Data
Pillars
People
Dynamic and Granular Access Control
Continuous Reevaluation of Trust
Compliant Configuration
Device Inventory
Integration of Asset Mgt. with Vulnerability Mgt. Tools
Zero Trust Device Compliance Monitoring
Continuous Device Posture Security Assessments
Dynamic Policy Safeguards
Cybersecurity Threat Hunt Capability Enhancements
Modernized Network
Enhanced User Experience
Improved Security Visibility
FedRAMP
Compliance to FedRAMP and IS2P
Cloud and Application Integration
Secured FDA Cloud Environments
AI and ML Support
Data Protection
Categorized and Inventoried Data
NDLP Implementation
Digital Rights Management Implementation
Supporting Pillars
Visibility & Analytics
Automation & Orchestration
Governance

PILLARS OF ZERO TRUST

Pillar 1: Identity. Implement strong Identity Credential and Access Management tools, principles, and multi-factor authentication to safeguard against identity spoofing, phishing, and unauthorized attempts to access our environments.

Pillar 2: Device. Implement technical capabilities to protect laptops, workstations, servers, smartphones, and tablets. Implement device inventory monitoring, dashboards, and endpoint detection and response for tracking purposes.

Pillar 3. Network Environment. Implement and modernize network security. Continue to reduce the potential attack surface and implement Software Defined Networks, modern cloud connections, network segmentation, and Secure Access Service Edge services.

Pillar 4: Application Workload. Enhance system and application monitoring capabilities to detect cyber threats and network and system outages. Secure applications using a model of never-trust and always-verify. Continue to advance cloud access security broker, adapt DevSecOps and threat intelligence capabilities to rigorously scan for security gaps and compliance with FISMA, FedRAMP, HHS, and other security requirements.

Pillar 5: Data. Safeguard FDA information against unauthorized disclosure, access, or misuse. Protect and encrypt data in transit and at rest. Enhance FDA's Data Loss Prevention capabilities to prevent exfiltration of sensitive data and enable and promote data sharing and collaboration.

Support Pillar 1: Visibility and Analytics. Provide visibility and data analytics for near real-time monitoring, searching, analyzing, and logging capabilities by utilizing FDA's next-generation Cybersecurity Platform. The platform integrates threat intelligence feeds with immersive dashboards and advanced analytical engines that, combined with real-time and historical data correlation services, make it possible to proactively and efficiently identify and respond to cybersecurity anomalies.

Support Pillar 2: Automation and Orchestration. Automate cybersecurity and network infrastructure events and transform them into actionable intelligence and supports secure workload automation enhancement through FDA's Cybersecurity Platform. Automation and orchestration refer to the programming that enables analysts to respond to threats from malicious actors promptly and allows them to focus their attention on cases rather than tasks.

Support Pillar 3: Governance. Provide governance support and enterprise alignment for FDA's Zero Trust activities through the FDA Cyber and Data Security Advisory Committee/Subcommittee and Technology Council under the guidance of the HHS CISO Council and other federal government security requirements. The FDA's Zero Trust approach aligns with our Cybersecurity Strategic Plan 2022- 2025, the NIST Special Publication 800-207, Zero Trust Architecture, Cybersecurity Framework, Risk Management Framework, and the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model.

FDA will measure progress and level of maturity using an FDA Zero Trust Scorecard based on criteria defined in the CISA Zero Trust Maturity Model outlined below:

Traditional. Manual configurations and assignment of attributes, static security policies, pillar-level solutions with coarse dependencies on external systems, least-function established at provisioning, proprietary and inflexible pillars of policy enforcement, manual incident response, and mitigation deployment.

Advanced. Some cross-pillar coordination, centralized visibility, centralized identity control, policy enforcement based on cross-pillar inputs and outputs, some incident response to pre-defined mitigations, increased detail in dependencies with external systems, and some least-privilege changes based on posture assessments.

Optimal. Fully automated assigning of attributes to assets and resources, dynamic policies based on automated/observed triggers, assets with self-enumerating dependencies for dynamic least privilege access, alignment with open standards for cross-pillar interoperability and centralized visibility with historical functionality for point-in-time recollection.

CYBERSECURITY, INNOVATION, AND TECHNOLOGY

ODT has prioritized cybersecurity innovation and modernization to formalize our commitment to technology and catalyze change to advance the mission of the FDA. Through the application of innovation management frameworks, we will identify, prioritize, and validate cybersecurity governance, standards, and solutions to support the secure adoption of emerging technologies such as Zero Trust and digital transformation across the Agency. These activities will drive and inform FDA's ongoing modernization efforts. We will continue to migrate to innovative tools and technologies like machine learning, AI, data sharing, collaboration platforms, and high-performance computing to advance FDA's public health mission. Innovation and emerging technologies underpin the advancement of patient-centered and real-world evidence-based regulatory operations.

Key Cybersecurity Modernization Actions

- Establish a comprehensive Zero Trust approach to facilitate new digital services and modernization efforts
- Promote software assurance best practices to include security measures at every stage of the development lifecycle
- Enhance interoperable and secure data exchange and collaboration across FDA and its public health partners
- Leverage Artificial Intelligence/Machine Learning (AI/ML) technologies to enhance cyber detection and response capabilities
- Integrate counterintelligence and insider risk principles with the Zero Trust model to enable an intelligence-driven approach
- Prioritize and invest in FDA's cybersecurity workforce

As the cyber threat landscape evolves globally, threat actors present ever-changing challenges. FDA will modernize our cyber defenses and continue to invest in and prioritize our cybersecurity workforce to meet current and future cybersecurity needs. Our workforce activities will focus on adopting new processes and technologies to create a highly skilled workforce.

As a "mission first, people always" organization, we will sustain the professional development and skills across our program and have aligned our cyber workforce objectives with Presidential Executive Order 13870 *America's Cybersecurity Workforce*. These efforts also align with the NIST National Initiative for Cybersecurity Education (NICE), targeting skillsets necessary for cyber innovation. Our Cybersecurity, Counterintelligence, and Insider Threat Program will enhance recruitment, hiring, and retention plans to meet our next-generation cyber needs and modernization objectives.

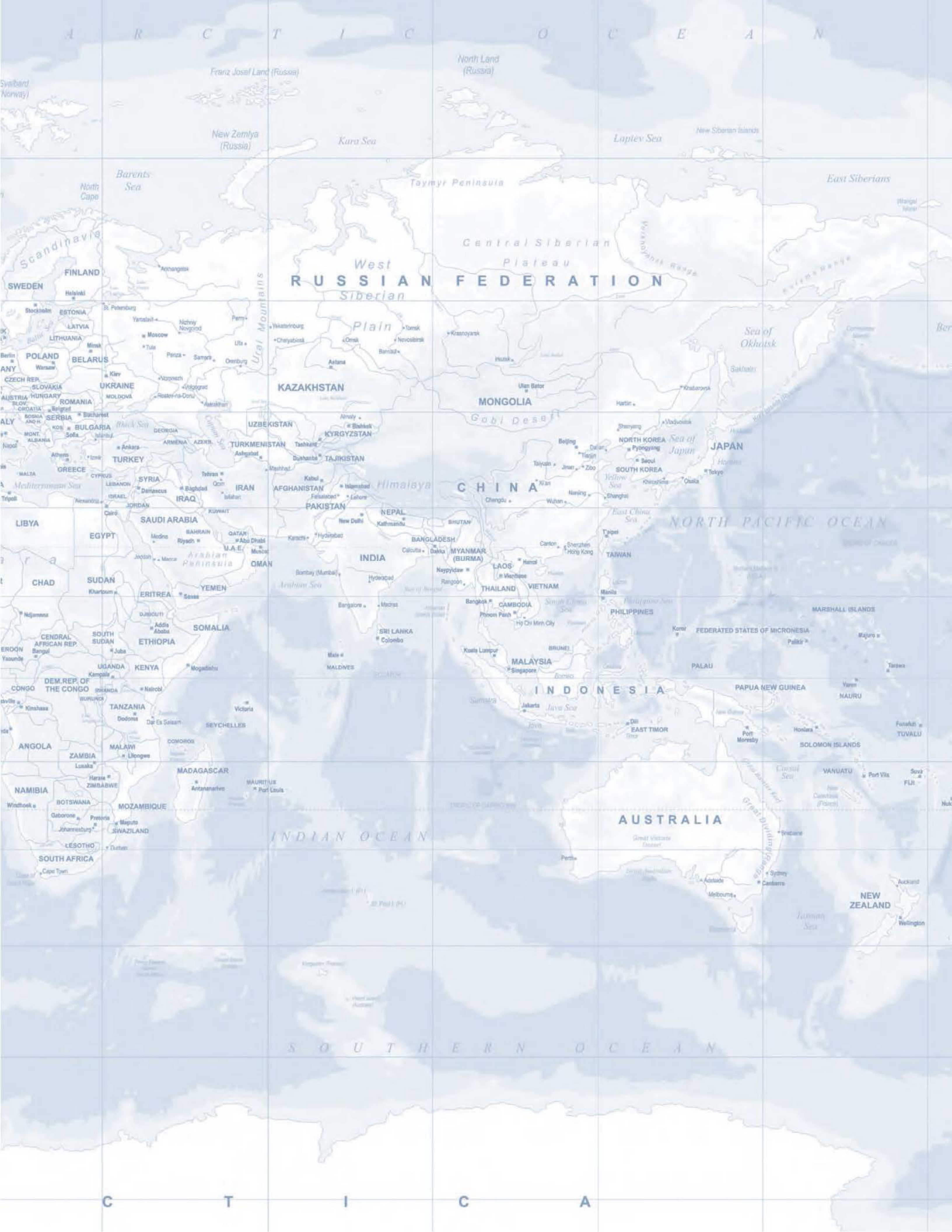
CONCLUSION

This CMAP outlines an approach to attain an optimal maturity level by modernizing and enhancing our security and cyber defenses to address evolving cyber threats, vulnerabilities, and risks to the FDA's IT infrastructure and sensitive data.

Our future vision is a highly skilled cyber workforce that leverages state-of-the-art technologies and advanced processes to address the challenges of a highly evolving threat landscape. Adopting this Zero Trust approach will serve as an added layer of protection to the FDA's digital environment. It will create opportunities for enhancements across the enterprise resulting in specific improvements, including but not limited to the following:

- Improved Customer Experience
- Increased Performance
- Enhanced Visibility and Situational Awareness
- Enhanced Threat Protections
- Reduced Latency and Speed to the Cloud

Strengthening FDA's network environment, identity capabilities, and data protections are critical as the Agency continues to modernize and deploy new digital services and facilitate more seamless data sharing across its global regulatory environment. Our CMAP will support the Agency in building a modern security architecture that will expedite digital transformation and directly support FDA's mission to protect and promote U.S. public health.


A R C T I C O C E A N
Franz Josef Land (Russia)
North Land (Russia)
Svalbard (Norway)
New Zemlya (Russia)
Kara Sea
Laptev Sea
New Siberian Islands
Barents Sea
North Cape
Taymyr Peninsula
East Siberians
Wrangel Island
Scandinavia
Central Siberian Plateau
West Siberian Plain
RUSSIAN FEDERATION
Ural Mountains
Verkhoyansk Range
Kolyma Range
FINLAND
SWEDEN
Helsinki
Arkhangelsk
Stockholm
ESTONIA
St. Petersburg
LATVIA
LITHUANIA
Yaroslavl
Nizhniy Novgorod
Perm
Yekaterinburg
Tomsk
Krasnoyarsk
Moscow
Chelyabinsk
Omsk
Novosibirsk
Minsk
Tula
Ufa
Barnaul
Sea of Okhotsk
Berlin
POLAND
BELARUS
Warsaw
Penza
Samara
Orenburg
Astana
Irkutsk
Lake Baikal
Sakhalin
GERMANY
CZECH REP.
Kiev
Voronezh
SLOVAKIA
UKRAINE
Volgograd
KAZAKHSTAN
Ulan Bator
Khabarovsk
AUSTRIA
HUNGARY
MOLDOVA
Rostov-na-Donu
SLOV.
ROMANIA
Astrakhan
MONGOLIA
CROATIA
Belgrad
Harbin
ITALY
BOSNIA AND H.
SERBIA
Bucharest
Black Sea
Caspian Sea
UZBEKISTAN
Almaty
Gobi Desert
Vladivostok
MONT.
KOS.
BULGARIA
GEORGIA
Bishkek
Shenyang
ALBANIA
Sofia
Istanbul
KYRGYZSTAN
Napoli
ARMENIA
AZERB.
TURKMENISTAN
Tashkent
Beijing
Dalian
NORTH KOREA
Sea of Japan
Ankara
Ashgabat
Tianjin
Pyongyang
JAPAN
Athens
Izmir
TURKEY
Dushanbe
TAJIKISTAN
Taiyuan
Jinan
Zibo
Seoul
Honshu
GREECE
Mashhad
SOUTH KOREA
Tokyo
MALTA
CYPRUS
Tehran
Kabul
Yellow Sea
Kitakyushu
Osaka
Mediterranean Sea
LEBANON
SYRIA
Qom
IRAN
AFGHANISTAN
Islamabad
Himalaya
CHINA
Xi'an
Nanjing
Shanghai
Tripoli
ISRAEL
Damascus
Baghdad
Isfahan
Faisalabad
Lahore
Chengdu
Wuhan
Alexandria
JORDAN
IRAQ
PAKISTAN
Cairo
KUWAIT
NEPAL
East China Sea
LIBYA
SAUDI ARABIA
BAHRAIN
New Delhi
Kathmandu
BHUTAN
Taipei
NORTH PACIFIC OCEAN
EGYPT
Medina
Riyadh
QATAR
Abu Dhabi
Karachi
Hyderabad
BANGLADESH
Canton
Shenzhen
Hong Kong
U.A.E.
Muscat
Calcutta
Dakka
MYANMAR (BURMA)
TAIWAN
Sahara
Jeddah
Mecca
Arabian Peninsula
OMAN
INDIA
LAOS
Hanoi
Bombay (Mumbai)
Naypyidaw
Vientiane
CHAD
SUDAN
Hyderabad
Rangoon
Khartoum
YEMEN
Arabian Sea
THAILAND
VIETNAM
ERITREA
Sanaa
Bay of Bengal
Luzon
Manila
Philippine Sea
Bangalore
Madras
Bangkok
CAMBODIA
South China Sea
N'djamena
DJIBOUTI
Andaman Islands (India)
Phnom Penh
PHILIPPINES
MARSHALL ISLANDS
Addis Ababa
SOMALIA
SRI LANKA
Ho Chi Minh City
CENTRAL AFRICAN REP.
SOUTH SUDAN
ETHIOPIA
Colombo
Koror
FEDERATED STATES OF MICRONESIA
Majuro
Palikir
CAMEROON
Bangui
Juba
Kuala Lumpur
BRUNEI
Yaounde
Male
MALAYSIA
UGANDA
KENYA
Mogadishu
MALDIVES
Singapore
PALAU
Tarawa
Kampala
Borneo
DEM. REP. OF THE CONGO
CONGO
RWANDA
Nairobi
Yaren
NAURU
PAPUA NEW GUINEA
BURUNDI
INDONESIA
Brazzaville
Kinshasa
TANZANIA
Victoria
Sumatra
Jakarta
Java Sea
Dodoma
Dar Es Salaam
SEYCHELLES
Java
Dili
EAST TIMOR
Port Moresby
Honiara
Funafuti
TUVALU
Luanda
ANGOLA
MALAWI
COMOROS
SOLOMON ISLANDS
ZAMBIA
Lilongwe
Lusaka
MADAGASCAR
Coral Sea
VANUATU
Port Vila
Suva
FIJI
NAMIBIA
Harare
ZIMBABWE
Antananarivo
MAURITIUS
Port Louis
Windhoek
BOTSWANA
MOZAMBIQUE
Great Barrier Reef
New Caledonia (France)
Gaborone
Pretoria
Maputo
Tropic of Capricorn
AUSTRALIA
Johannesburg
SWAZILAND
Great Dividing Range
Brisbane
INDIAN OCEAN
Great Victoria Desert
LESOTHO
Durban
SOUTH AFRICA
Perth
Cape Town
Great Australian Bight
Adelaide
Sydney
Canberra
Melbourne
Auckland
NEW ZEALAND
Wellington
Tasman Sea
Tasmania
Kerguelen (France)
Heard Island (Australia)
S O U T H E R N O C E A N
C T I C A

OFFICE OF INFORMATION SECURITY
OFFICE OF DIGITAL TRANSFORMATION