DEPARTMENT of HEALTH and HUMAN SERVICES

Fiscal Year 2024

Public Health and Social Services Emergency Fund

Justification of Estimates for Appropriations Committee

We are pleased to present the Fiscal Year (FY) 2024 Congressional Justification for the Public Health and Social Services Emergency Fund (PHSSEF). The FY 2024 Budget Request directly supports the United States' ability to prepare for, respond to, and recover from the consequences of a wide range of natural and man-made medical and public health security threats and includes the FY 2024 budget justification for the HHS Office of the Chief Information Officer Cybersecurity Program, the Office of National Security (ONS), the Office of Global Affairs (OGA) pandemic programs, the U.S. Public Health Service Commissioned Corps led by the Office of the Assistant Secretary for Health (OASH), and other HHS-wide preparedness proposals. The FY 2024 Budget requests resources for the Administration for Strategic Preparedness and Response (ASPR) in a new account, separate from PHSSEF where funding has historically been appropriated. Please see the ASPR Congressional Justification for details on the FY 2024 Budget request.

Cybersecurity

The HHS Cybersecurity program maintains the security of an array of unique systems and sensitive data within the Department. To meet its mission, HHS maintains a vast array of secure information. The Department awards more grants than any other Federal agency, requiring systems in place to keep such financial data secure. Additionally, the Department's systems are utilized across the Federal Government and maintain sensitive data, including personally identifiable information, health records, sensitive biodefense research, and proprietary data.

The evolving cyber threat landscape coupled with the rapid proliferation of information assets due to the COVID-19 pandemic, the increased mobility of the HHS workforce, and the need to derive value and intelligence from information assets has forced HHS to redefine its approach to managing and protecting information assets. The Cybersecurity program plays a key role in the security and privacy of HHS Protect and its respective sub-component systems, including information stored, processed, and transmitted.

The FY 2023 President's Budget for the HHS Cybersecurity program is $188,326,000, which is $88,326,000 above FY 2023 Enacted. The FY 2024 request will allow HHS to manage existing solutions, address cybersecurity mandates through targeted initiatives, and complement current network protection tools. The requested funds continue support and sustainment of the Department's existing cybersecurity and privacy programs while also enabling deployment of cybersecurity initiatives aligned to the HHS priorities. In addition to the existing and emerging priorities supported by the cybersecurity program, requested funding provides support for the implementation of Zero Trust, improvement of multifactor authentication and encryption, improved logging, and expanding support of the Health and Public Health sector. These activities are mandated by Executive Orders, Office of Management and Budget memoranda, and law.

Office of National Security

The Office of National Security (ONS) provides strategic all-source information, intelligence, defensive counterintelligence, insider threat, cyber threat intelligence, enterprise supply chain risk management (E-SCRM), security for classified information, and communications security support across the Department. ONS increases the Department's security and threat awareness and its ability to respond swiftly and effectively to national and homeland security threats. ONS engages with Federal partners and others to analyze all-source intelligence/information and identify potential threats and vulnerabilities, and it identifies and assesses trends and patterns across the Department while developing and implementing

mitigation strategies. ONS is responsible for the safeguarding of all classified information, equipment, and facilities across the Department and is HHS's Federal Intelligence Coordination Office and the Secretary's Senior Intelligence Official. The FY 2024 President's Budget for ONS is $11,983,000, which is $3,000,000 above the FY 2023 Enacted.

U.S. Public Health Service Commissioned Corps

The United States Public Health Service Commissioned Corps (Corps) is a cadre of full-time and part time officers dedicated to promoting and advancing public health and disease prevention programs. As one of America's seven uniformed services, the Corps fills essential public health leadership and service roles within the nation's federal government agencies and programs.

Officers serve as physicians, nurses, pharmacists, dentists, dietitians, engineers, environmental health officers, health service officers, scientists, therapists, and veterinarians. In addition to their regular duties such as providing patient care to underserved populations or conducting biomedical research, Corps officers respond to public health crises, natural disasters, disease outbreaks, and terrorist attacks and serve on humanitarian assistance missions around the world. To protect the health of the American people for the next century, the Corps has engaged in an historic modernization initiative that will transform its force structure and ensure its readiness in order to meet the full spectrum of public health challenges facing the nation.

The FY 2024 budget provides $20 million for the Office of the Assistant Secretary for Health within the Office of the Secretary. This funding will provide for the Commissioned Corps of the U.S. Public Health Service. These new resources will support:

- $2 million for U.S. Public Health Service Readiness and Training activities,
- $4 million for the Public Health and Emergency Response Strike Team, and
- $14 million for Commissioned Corps Ready Reserve.

These investments will ensure the Commissioned Corps is equipped to effectively respond to future public health emergency response operations, as rapidly as possible, while being equipped with surge capacity.

Office of Global Affairs Influenza and Pandemic Negotiation

The PHSSEF supports the HHS Office of Global Affairs in their work to lead global health diplomacy and policy coordination efforts for HHS to strengthen international pandemic preparedness, especially pandemic influenza preparedness. OGA will continue to enhance international influenza preparedness by providing strategic coordination and technical expertise on health policy development and diplomacy to global partners, including nearly 200 Ministries of Health.

Pandemic Preparedness Mandatory Funding

The budget includes $20 billion in mandatory funding, available over five years, across the Administration for Strategic Preparedness and Response (ASPR), Centers for Disease Control and Prevention (CDC), National Institutes of Health (NIH), and the Food and Drug Administration (FDA) in support of pandemic preparedness and biodefense priorities as outlined in the *2021 American Pandemic Preparedness Plan* and the *2022 National Biodefense Strategy and Implementation Plan*.

Public Health Emergency Fund

The FY 2024 Budget provides $50 million for the Public Health Emergency Fund, authorized by section 319(b) of the Public Health Service Act, to allow the HHS Secretary to immediately respond to a public health threat or declared emergency. These flexible funds are available to address the breadth of the Department's responsibilities and will allow HHS to rapidly deploy resources early in a response effort. Potential uses for the funding include deploying human services resources after a natural disaster, responding to the public health effects of a terrorist attack, addressing emergency nutritional needs for vulnerable populations, or responding to any other public health threat.

Secretary's 1% Transfer Authority

The FY 2024 President's Budget proposes to expand the HHS Secretary's one percent transfer authority such that the PHSSEF appropriation could be increased by up to ten percent instead of three percent. As learned from public health threats such as COVID-19, it is critical for the Department to have the flexibility needed to respond as quickly as possible when such threats arise. An expanded one percent transfer authority would allow the Secretary to transfer more resources to emergency programs funded by the PHSSEF appropriation in order to accelerate critical public health and medical response activities.

Andrea Palm
HHS Deputy Secretary

Karl Mathias
HHS Chief Information Security Officer

Robert Rohrer
Acting Assistant Deputy Secretary for National Security

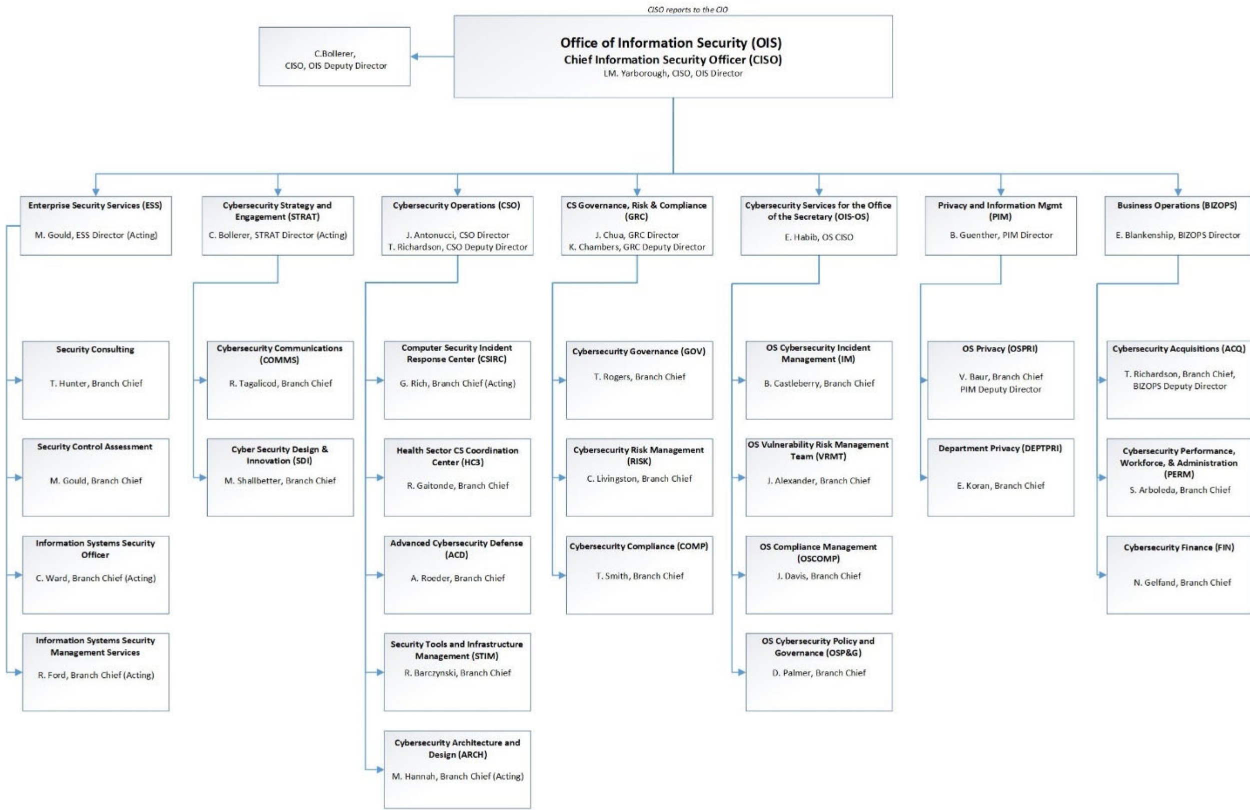
Contents

Organizational Charts ... 6
Assistant Secretary for Administration (ASA) ... 6
    Cybersecurity ... 6
    Office of National Security ... 7
Introduction and Mission ... 8
Overview of Budget Request ... 9
All Purpose Table ... 11
Appropriations Language ... 12
    FY 2024 Appropriations Language ... 12
    FY 2024 General Provision ... 14
    Appropriations Language Analysis ... 15
Amounts Available for Obligation ... 17
Summary of Changes ... 18
Budget Authority by Activity ... 19
Authorizing Legislation ... 20
Appropriations History ... 21
Appropriations Not Authorized by Law ... 23
Office of Global Affairs ... 24
Assistant Secretary for Administration ... 28
    Cybersecurity ... 28
Immediate Office of the Secretary ... 40
    Office of National Security ... 40
Assistant Secretary for Health ... 44
    Commissioned Corps Readiness Training ... 44
    U.S. Public Health Service Ready Reserve ... 46
    Public Health and Emergency Response Strike Team ... 49
Public Health Emergency Fund ... 51
Pandemic Preparedness ... 53
Overview of Preparedness Legislative Proposals ... 61
Nonrecurring Expenses Fund ... 68
    Office of National Security ... 68
IDEA Digital Modernization Act ... 69
Supplemental Material ... 70
    Budget Authority by Object Class ... 70
    Salaries and Expenses ... 71
    Detail of Full-Time Equivalent Employment ... 72
    Detail of Positions ... 73
    Programs Proposed for Elimination ... 74

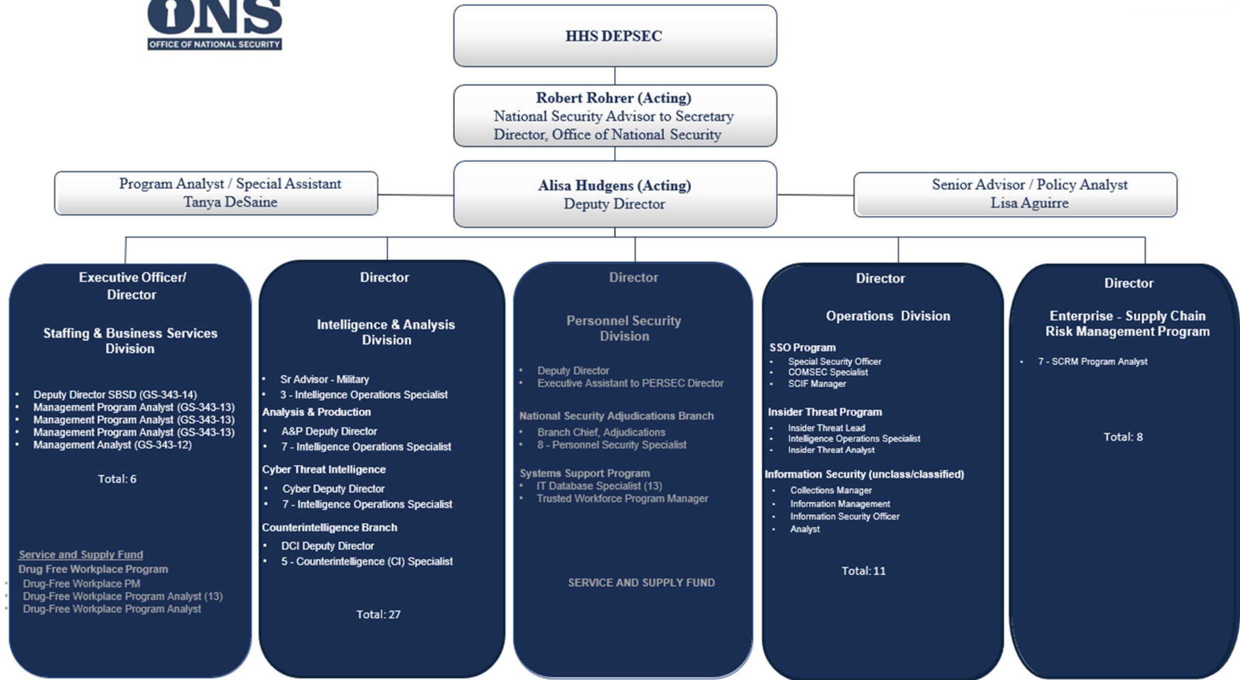
ORGANIZATIONAL CHARTS

ASSISTANT SECRETARY FOR ADMINISTRATION (ASA)

Cybersecurity



Office of National Security



INTRODUCTION AND MISSION

The Public Health and Social Services Emergency Fund supports the Department's cross-cutting efforts to improve the Nation's preparedness and response against naturally occurring and man-made health threats and threats to the ability of HHS to carry out such missions. The following programs are supported by this Fund:

Cybersecurity

The Cybersecurity program, within the Office of the Assistant Secretary for Administration (ASA), Office of the Chief Information Officer (OCIO), coordinates the Department's cybersecurity efforts and provides enterprise level program management and oversight. The program works to ensure that the automated information systems are designed, operated, and maintained with the appropriate information technology security and privacy data protections.

Office of National Security

The Office of National Security (ONS) provides strategic all-source information, intelligence, defensive counterintelligence, insider threat, cyber threat intelligence, enterprise supply chain risk management (E-SCRM), security for classified information, and communications security support across the Department.

U.S. Public Health Service Commissioned Corps

The United States Public Health Service Commissioned Corps (Corps) is a cadre of full-time and part-time officers dedicated to promoting and advancing public health and disease prevention programs. As one of America's seven uniformed services, the Corps fills essential public health leadership and service roles within the Nation's Federal Government agencies and programs.

Office of Global Affairs Influenza and Pandemic Negotiation

As part of the PHSSEF, the Office of Global Affairs (OGA) leads global health diplomacy and policy coordination efforts for HHS to strengthen international pandemic preparedness, especially pandemic influenza preparedness

OVERVIEW OF BUDGET REQUEST

The discretionary FY 2024 President's Budget for the Public Health and Social Services Emergency Fund (PHSSEF) is $278,318,000, which is an increase of +$162,326,000 above FY 2023 enacted[1]. Additionally, the FY 2024 President's Budget includes a request for $20,000,000,000 in mandatory funding as part of a department-wide plan to prepare for future pandemics and other biological threats. This mandatory pandemic preparedness funding is requested within the PHSSEF but will be allocated across the Administration for Strategic Preparedness and Response, the Centers for Disease Control and Prevention, the National Institutes of Health, and the Food Drug Administration. The FY 2024 request for PHSSEF will provide the necessary resources to:

- Support a cross-agency effort to carry out priorities for national pandemic preparedness and biodefense;
- Support the Department's counter-intelligence program;
- Support the Department's cybersecurity efforts;
- Support the Department's pandemic influenza preparedness and response activities;
- Support U.S. Public Health Service Commissioned Corps training, reserve staffing, and rapid deployments; and
- Fund the Public Health Emergency Fund that the Secretary of HHS can deploy in response to a declared or potential public health emergency.

The Budget provides funds for programs within the Office of the Secretary, specifically for the Office of the Assistant Secretary for Administration (ASA), the Office of National Security (ONS), the Office of the Assistant Secretary for Health (OASH), funding for pandemic preparedness activities within the Office of Global Affairs (OGA), and for the Public Health Emergency Fund (PHEF).

Programmatic Increases (relative to the FY 2023 Omnibus):

Pandemic Preparedness (mandatory): $20 billion in mandatory funding, available for a period of five years, to support the Administration's pandemic preparedness and biodefense priorities across ASPR, CDC, NIH, and FDA. Funding will transform the Nation's capabilities to prepare for and respond rapidly and effectively to future pandemics and other high consequence biological threats.

Cybersecurity (increase of +$88.326 million, $188.326 million total): The FY 2024 request will allow HHS to manage existing solutions, address cybersecurity mandates through targeted initiatives, and complement current network protection tools. The requested funds continue support and sustainment of the HHS's existing cybersecurity and privacy programs while also enabling deployment of cybersecurity initiatives aligned to the HHS's cybersecurity priorities In addition to the existing and emerging priorities supported by the cybersecurity program, requested funding provides support for the implementation of Zero Trust Architecture, improvement of Multifactor Authentication and encryption, improved logging, and expanding support of the Healthcare and Public Health sector

Public Health Emergency Fund (new program, $50 million total): The FY 2024 budget provides $50 million for the Public Health Emergency Fund, authorized by section 319(b) of the Public Health

[1] In FY 2023, the PHSSEF appropriation included funding for the Administration for Strategic Preparedness and Response (ASPR). For FY 2024, the budget requests that ASPR receive its own direct appropriation. The budget levels here and elsewhere throughout this document have been comparably adjusted to remove ASPR funding amounts.

Service Act, to allow the HHS Secretary to immediately respond to a public health threat or declared emergency. These flexible funds are available to address the breadth of the Department's responsibilities and will allow HHS to mobilize and rapidly deploy resources early in a response effort. Potential uses for the funding include deploying human services resources such as emergency nutritional support for vulnerable populations, responding to the public health effects of a terrorist attack, or responding to any other public health threat. The Public Health Emergency Fund last received an appropriation in 1993.

Office of the Assistant Secretary for Health (increase of +$20 million, $20 million total): The Budget requests $20 million for the U.S. Public Health Service Commissioned Corps to continue readiness and training programs supported by COVID-19 supplemental appropriations. Funds will be used to: ensure the Corps is fully trained and ready to respond to any number of public health and medical emergencies; support a dedicated strike team of Active Duty Corps Officers to immediately respond to emergent situations; and continue to build and support a ready reserve of Corps Officers.

Office of National Security (increase of +3 million, $11.983 million total): The FY 2024 President's Budget supports the ability of ONS to further protect the Department against insider security threats, conduct Cyber Threat analysis, protect sensitive unclassified and classified information, and allow ONS to fully develop the newly established Enterprise Supply Chain Risk Management Program.

Office of Global Affairs (increase of +$1 million, $8.009 million total): The budget supports OGA's pandemic preparedness work, which includes leading global health diplomacy and policy coordination efforts for HHS to strengthen international pandemic preparedness, especially pandemic influenza preparedness. The increase in funds will be used to support negotiations with the World Health Organization on a pandemic preparedness instrument.

ALL PURPOSE TABLE

(Dollars in Millions)

Activity	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget		FY 2024 President's Budget +/- FY 2023 Enacted
			Funding	FTEs	Funding
Office of the Secretary:					
Office of Global Affairs (OGA)	7.009	7.009	8.009	20	+1.000
Pandemic Influenza	*7.009*	*7.009*	*7.009*	*18*	--
Pandemic Negotiators	--	--	*1.000*	*2*	*+1.000*
Cybersecurity (OCIO)	71.415	100.000	188.326	143	+88.326
Office of National Security (ONS)	8.510	8.983	11.983	56	+3.000
Office of the Assistant Secretary for Health (OASH)	--	--	20.000	157	+20.000
USPHS Readiness & Training	--	--	*2.000*	*2*	*+2.000*
Public Health and Emergency Response Strike Team	--	--	*4.400*	*24*	*+4.400*
Commissioned Corps Ready Reserve	--	--	*13.600*	*131*	*+13.600*
Public Health Emergency Fund /1	--	--	50.000	--	+50.000
Total, PHSSEF, Budget Authority	**86.934**	**115.992**	**278.318**	**376**	+162.326
Pandemic Preparedness (Mandatory) /2	--	--	20,000.000	--	+20,000.000
Total, PHSSEF Program Level	**86.934**	**115.992**	**20,278.318**	**376**	+20,162.326

Note: The Public Health and Social Services Fund previously contained the annual appropriation for the Administration for Strategic Preparedness and Response (ASPR). The FY 2024 budget requests funding for ASPR in a separate, new appropriation account. This table is comparably adjusted to remove ASPR's programs from FY 2022 and FY 2023.

1/ To be deposited in the Public Health Emergency Fund as authorized in section 319(b) of the PHS Act.
2/ Reflects mandatory funding to be allocated across ASPR, CDC, NIH, and FDA.

APPROPRIATIONS LANGUAGE

FY 2024 Appropriations Language

[For expenses necessary to support activities related to countering potential biological, nuclear, radiological, chemical, and cybersecurity threats to civilian populations, and for other public health emergencies, $1,647,569,000, of which $950,000,000 shall remain available through September 30, 2024, for expenses necessary to support advanced research and development pursuant to section 319L of the PHS Act and other administrative expenses of the Biomedical Advanced Research and Development Authority: *Provided,* That funds provided under this heading for the purpose of acquisition of security countermeasures shall be in addition to any other funds available for such purpose: *Provided further,* That products purchased with funds provided under this heading may, at the discretion of the Secretary, be deposited in the Strategic National Stockpile pursuant to section 319F–2 of the PHS Act: *Provided further,* That $5,000,000 of the amounts made available to support emergency operations shall remain available through September 30, 2025: *Provided further*, That $75,000,000 of the amounts made available to support coordination of the development, production, and distribution of vaccines, therapeutics, and other medical countermeasures shall remain available through September 30, 2024.

For expenses necessary for procuring security countermeasures (as defined in section 319F–2(c)(1)(B) of the PHS Act), $820,000,000, to remain available until expended.

For expenses necessary to carry out section 319F–2(a) of the PHS Act, $965,000,000, to remain available until expended.

For an additional amount for expenses necessary to prepare for or respond to an influenza pandemic, $335,000,000; of which $300,000,000 shall be available until expended, for activities including the development and purchase of vaccine, antivirals, necessary medical supplies, diagnostics, and other surveillance tools: *Provided,* That notwithstanding section 496(b) of the PHS Act, funds may be used for the construction or renovation of privately owned facilities for the production of pandemic influenza vaccines and other biologics, if the Secretary finds such construction or renovation necessary to secure sufficient supplies of such vaccines or biologics.]

For expenses necessary to carry out Title II of the PHS Act with respect to Commissioned Corps Readiness Training, Ready Reserves, and the Public Health Emergency Response Strike Team; to support, except as otherwise provided, activities related to safeguarding classified national security information and providing intelligence and national security support across the Department; and to counter cybersecurity threats to civilian populations, $220,309,000;

For an additional amount for expenses necessary to prepare for or respond to an influenza pandemic and to coordinate and participate in international negotiations on pandemic preparedness, prevention, and response, $8,009,000: Provided, That notwithstanding section 496(b) of the PHS Act, funds available for preparing for or responding to an influenza pandemic may be used for the construction or renovation of privately owned facilities for the production of pandemic influenza vaccines and other biologics, if the Secretary finds such construction or renovation necessary to secure sufficient supplies of such vaccines or biologics.

For an additional amount for deposit in the Public Health Emergency Fund established by section 319(b) of the PHS Act, $50,000,000, to remain available until expended: Provided, That the activities funded with amounts made available under this paragraph may include the acquisition of products for deposit

into the strategic national stockpile maintained under section 319F-2 of such Act: Provided further, That amounts made available in this paragraph in this Act may be used for the construction, alteration, or renovation of non-federally owned U.S.-based facilities for the production of medical countermeasures, including vaccines, therapeutics, diagnostics and other medical supplies, the development of medical countermeasures and supplies, and the end-to-end logistics associated with the distribution of such medical countermeasures and supplies where the Secretary determines that such actions are necessary to develop and secure sufficient amounts of such medical countermeasures and supplies: Provided further, That amounts made available in this paragraph in this Act may be transferred to, and merged with, the Covered Countermeasure Process Fund authorized by section 319F-4 of the PHS Act: Provided further, That the transfer authority provided in this paragraph in this Act is in addition to any other transfer authority provided by law: Provided further, That the Secretary shall notify the Committees on Appropriations of the House of Representatives and the Senate not later than 5 days after any obligation in excess of $5,000,000 is made from amounts made available in this paragraph in this Act.

FY 2024 General Provision

SEC. 234. For purposes of any transfer to appropriations under the heading "Department of Health and Human Services—Office of the Secretary—Public Health and Social Services Emergency Fund", section 204 of this Act shall be applied by substituting "10 percent" for "3 percent".

Appropriations Language Analysis

Language Provision	Explanation
For expenses necessary to carry out Title II of the PHS Act with respect to Commissioned Corps Readiness Training, Ready Reserves, and the Public Health Emergency Response Strike Team; to support, except as otherwise provided, activities related to safeguarding classified national security information and providing intelligence and national security support across the Department; and to counter cybersecurity threats to civilian populations, $220,309,000;	This topline language supports the programs that are retained in the PHSSEF after removing ASPR. The Office of National Security, HHS OCIO Cybersecurity Program, and the Commissioned Corps programs detailed in this document are supported from this paragraph.
For an additional amount for expenses necessary to prepare for or respond to an influenza pandemic and to coordinate and participate in international negotiations on pandemic preparedness, prevention, and response, $8,009,000: Provided, That notwithstanding section 496(b) of the PHS Act, funds available for preparing for or responding to an influenza pandemic may be used for the construction or renovation of privately owned facilities for the production of pandemic influenza vaccines and other biologics, if the Secretary finds such construction or renovation necessary to secure sufficient supplies of such vaccines or biologics.	This language is retained and slightly adapted from the FY 2023 PHSSEF appropriation language so that the Office of Global Affairs can continue to perform their pandemic preparedness activities. Additionally, the scope is expanded so that OGA can support pandemic negotiation work.
For an additional amount for deposit in the Public Health Emergency Fund established by section 319(b) of the PHS Act, $50,000,000, to remain available until expended: Provided, That the activities funded with amounts made available under this paragraph may include the acquisition of products for deposit into the strategic national stockpile maintained under section 319F-2 of such Act: Provided further, That amounts made available in this paragraph in this Act may be used for the construction, alteration, or renovation of non-federally owned U.S.-based facilities for the production of medical countermeasures, including vaccines, therapeutics, diagnostics and other medical supplies, the development of medical countermeasures and supplies, and the end-to-end logistics associated with the distribution of such medical countermeasures and supplies where the Secretary determines that such actions are necessary to develop and secure sufficient amounts of such medical countermeasures and supplies: Provided further, That amounts made available in this paragraph in this Act may be transferred to, and merged with, the Covered Countermeasure Process Fund authorized by section 319F-4 of the PHS Act: Provided further, That the transfer authority provided in this paragraph in this Act is in addition to any other transfer authority provided by law: Provided further, That the Secretary shall notify the Committees on Appropriations of the House of Representatives and the Senate not later than 5 days after any obligation in excess of $5,000,000 is made from amounts made available in this paragraph in this Act:	This paragraph appropriates $50 million to the Public Health Emergency Fund established by section 319(b) of the PHS Act. It also establishes transfer authority to the Cover Countermeasure Process Fund and establishes a reporting requirement related to obligations.

For purposes of any transfer to appropriations under the heading "Department of Health and Human Services—Office of the Secretary—Public Health and Social Services Emergency Fund", section 204 of this Act shall be applied by substituting "10 percent" for "3 percent".	This language expands the Secretary's one percent transfer authority in Section 204 of the Public Health Service Act such that the PHSSEF appropriation could be increased by up to ten percent instead of three percent. Building on lessons learned from the COVID-19 pandemic response, an expanded Secretary's one percent transfer authority would provide additional flexibility for the Department during a public health emergency to accelerate critical activities funded by the PHSSEF appropriation.

AMOUNTS AVAILABLE FOR OBLIGATION

Detail	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget
Appropriation	$3,199,678,000	$3,767,569,000	$278,318,000
Supplemental (P.L. 117-159)	$82,000,000	$32,000,000	$0
Supplemental (P.L. 117-328)	$0	$128,792,000	$0
Subtotal, Adjusted Appropriation	**$3,281,678,000**	**$3,928,361,000**	**$278,318,000**
Bipartisan Safer Communities Act			
Transfer of Funds to HRSA - Health Workforce	-$12,000,000	-$12,000,000	
Transfer of Funds to HRSA - Maternal and Child Health	-$20,000,000	-$20,000,000	
Transfer of Funds to CMS - Grants to States for Medicaid	-$50,000,000	$0	
Disaster Relief Supplemental Appropriations Act, 2023			
Transfer of Funds to HRSA - Primary Health Care	$0	-$65,000,000	
Transfer of Funds to SAMHSA - Health Surveillance and Program Support	$0	-$22,000,000	
Transfer of Funds to ACL - Aging and Disability Services Programs	$0	-$15,000,000	
Transfer of Funds to FDA - Buildings and Facilities	$0	-$392,000	
Transfer of Funds to HHS-Office of Inspector General	$0	-$2,000,000	
Subtotal, Adjusted Budget Authority	**$3,199,678,000**	**$3,791,969,000**	**$278,318,000**
Unobligated balance, start of year	$95,726,685,888	$25,233,502,421	
Unobligated balance, end of year	$25,126,866,590		
Unobligated balance, lapsing	$106,635,832		
Unobligated balance transferred to CDC-wide Activities and Program Support	-$200,000,000		
Unobligated balance transferred from CDC-wide Activities and Program Support	$200,000,000		
Unobligated balance transferred to HRSA Covered Countermeasure Process Fund	-$4,270,381		
Total obligations	**$80,749,361,827**		

1. Excludes the following amounts for reimbursable activities carried out by this account: 2022 obligations $101,216,131.93
2. For columns FY 2022 and FY 2023, this exhibit includes funds appropriated to the PHSSEF but made available to ASPR. The FY 2024 column does not include ASPR's budget request, which is reflected in the ASPR Congressional Justification.

SUMMARY OF CHANGES

(Dollars in Millions)

2023 Enacted	
Total Budget Authority	$115.992
2024 President's Budget	
Total Estimated Budget Authority	$278.318
Net Change	+$162.326

	FY 2023 Enacted		FY 2024 President's Budget		FY 2024 +/- FY 2023	
Increases:	**BA**	**FTE**	**PB BA**	**PB FTE**	**BA**	**FTE**
Office of National Security	8.983	38	11.983	56	+3.000	+18
Office of Global Affairs	7.009	18	8.009	20	+1.000	+2
Cybersecurity	100.000	143	188.326	143	+88.326	--
Office of the Assistant Secretary for Health	--	--	20.000	157	+20.000	+157
Public Health Emergency Fund	--	--	50.000	--	+50.000	--
Total	115.992	199	278.318	376	+162.326	+177
Decreases						
Total Decreases	--	--	--	--	--	--
Net Change					+162.326	+177

Note: This exhibit is comparably adjusted to exclude ASPR programs previously supported via the PHSSEF, and also excludes $21.9 million in FY 2023 for HHS Protect which was provided to CDC via the PHSSEF. The FY 2024 Budget proposes directly appropriating funding to CDC instead of PHSSEF for HHS Protect.

BUDGET AUTHORITY BY ACTIVITY

(Dollars in Millions)

Activity	**FY 2022 Final**	**FY 2023 Enacted**	**FY 2024 President's Budget**
Emergency Preparedness and Response	79.925	108.983	271.309
Pandemic Influenza	7.009	7.009	7.009
Total Budget Authority	**86.934**	**115.992**	**278.318**
FTE	**163**	**199**	**376**

Note: This table is comparably adjusted to remove funding provided to the Administration for Strategic Preparedness and Response via the PHSSEF in FY 2022 and FY 2023, and also to remove HHS Protect from FY 2023, which is being implemented by the CDC and reflected in its FY2024 submission.

AUTHORIZING LEGISLATION

(Dollars in Millions)

Activity	FY 2023 Amount Authorized	FY 2023 Amount Appropriated	FY 2024 Amount Authorized	FY 2024 President's Budget
Pandemic Influenza	**250.000**	**287.000**	**NA**	**382.000**

Note: These amounts correspond to the Pandemic Influenza Program at ASPR and at HHS Office of Global Affairs, which were previously both funded through the PHSSEF. The FY 2024 budget requests funding for ASPR in a separate, new appropriation account. Funding for the Office of Global Affairs pandemic influenza activities in FY 2023 enacted and the FY 2024 budget is $7.009 million.

APPROPRIATIONS HISTORY

(Dollars in millions)

Details	Budget Estimate to Congress	House Allowance	Senate Allowance	Appropriation
FY 2015				
Appropriation			1,389.813	1,233.069
Supplemental Appropriation				733.000
Subtotal			1,389.813	1,966.069
				FY 2016
Appropriation	1,909.981			1,532.958
Supplemental Appropriation (PL 114-223)				387.000
Transfer to CMS				(75.000)
Transfer to HRSA				(66.000)
Transfer to OIG				(0.500)
Transfer to GAO				(0.500)
Subtotal	1,909.981			1,777.958
FY 2017				
Appropriation	1,431.117	1,631.258	1,517.958	1,532.958
Transfer to ACF				(3.520)
Subtotal	1,431.117	1,631.258	1,517.958	1,529.438
FY 2018				
Appropriation	1,662.616	1,739.258	1,552.958	1,953.458
Supplemental Appropriation (PL 115-123)				162.000
Transfer to HRSA				(60.000)
Transfer to SAMHSA				(20.000)
Transfer to OIG				(2.000)
Subtotal				2,033.458
FY 2019				
Appropriation	2,303.877	2,046.458	2,813.128	2,021.458
Transfer from CDC /1				610.000
Subtotal	2,303.877	2,046.458	2,813.128	2,631.458
FY 2020				
Appropriation	2,666.591	3,008.458	2,642.458	2,737.458
Supplemental Appropriation (PL 116-94)				535.000
Supplemental Appropriation (PL 116-123)				3,400.000
Transfer to OIG				(2.000)
Transfer to HRSA				(100.000)
Supplemental Appropriation (PL 116-127)				1,000.000
Supplemental Appropriation (PL 116-136)				127,274.500
Transfer to HRSA				(275.612)
Transfer to DHS				(289.000)
Transfer to OIG				(4.000)
Supplemental Appropriation (PL 116-139)				96,566.000

FY 2021				
Appropriation	2,641.465	2,827.458	2,913.458	2,847.458
Supplemental Appropriation (PL 116-260)				48,345.000
Transfer to IHS				(790.000)
Mandatory Funding (PL 117-02)				70,110.000
FY 2022				
Continuing Resolution (P.L. 117-86)				2,847.458
FY 2023				
Appropriation	3,814.610	3,699.356	3,629.479	3,767.569
Supplemental Appropriation (P.L. 117-159)				82.000
Supplemental Appropriation (P.L. 117-328)				128.792
FY 2024 /2				
Appropriation	278.318			

APPROPRIATIONS NOT AUTHORIZED BY LAW

(Dollars in Millions)

Program	Last Year of Authorization	Authorization Level	Appropriations in Last Year of Authorization	Appropriations in FY 2023
Cybersecurity	N/A	N/A	N/A	100.000
Office of National Security	N/A	N/A	N/A	8.983

OFFICE OF GLOBAL AFFAIRS

Budget Summary
(Dollars in Millions)

Office of Global Affairs	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2024 +/- FY 2023
Budget Authority	**7.009**	**7.009**	**8.009**	**+1.000**
FTE	**16**	**18**	**20**	**+2**

Authorizing Legislation ....Reorganization Plan No. 1 of 1953
FY 2024 Authorization ....Indefinite
Allocation Method .... Direct Federal

Program Description

OGA serves a unique role within HHS by providing leadership in global health diplomacy, fostering critical international relationships, providing strategic coordination for international health engagements across HHS and the U.S. Government (USG), and utilizing its expertise in global health and emerging infectious diseases for the development of policy. OGA synthesizes, integrates, and translates policy, science, and diplomatic issues and challenges into actionable steps and initiatives that support core principles (e.g., equity, accountability, transparency) and achieve progress on priorities for HHS, as well as for the many global partners with whom we work, including on international issues that impact or may be impacted by U.S. domestic considerations. On behalf of the Secretary, OGA manages key relationships with: nearly 200 Ministries of Health across the globe; key multilateral and international institutions involved in health security [e.g., the United Nations (World Health Organization [WHO], and Food and Animal Organization), the World Bank Group, the World Organization for Animal Health, the Association of Southeast Asian Nations, Organization of Islamic Cooperation, etc.]; and with numerous foreign governments (including through partnerships in the G7 and G20), particularly in developing countries. Working to strengthen U.S. health security through USG-wide and international engagement, OGA serves as a critical interface with international health, science, foreign policy and diplomacy, and security partners and programs that address influenza and other global health security and pandemic threats. Building on lessons learned from influenza preparedness and response efforts over the past twenty years and from the experience with other health security threats, OGA provides essential policy development support and coordinated diplomatic outreach to bolster global health security and equity, inform domestic preparedness and response efforts, and strengthen and expand partnerships that are crucial to face the challenges of influenza pandemic threats, and other emerging infectious disease threats of global concern.

The accomplishments from the HHS/Office of the Secretary International Pandemic Influenza funds have substantially advanced USG global health security priorities and U.S. foreign policy goals, elevating global prioritization of influenza preparedness, while supporting HHS programs to better prepare for preparing for seasonal influenza epidemics, the next influenza pandemic, and other pandemic threats.

Budget Request

OGA's FY 2024 request is $8,009,000, which is an increase of +$1,000,000 above FY 2023 Enacted. The additional Pandemic Influenza budget authority funds will allow the Office of Global Affairs to continue to provide leadership, technical expertise, oversight, policy and program coordination, and global health diplomacy to advance global health security, prioritizing preparedness for influenza pandemics, seasonal influenza epidemics, and other emerging infectious disease (EID) threats.

In accordance with the *National Security Strategy, the National Biodefense Strategy, the Global Health Security Strategy, the Global Health Security Agenda 2024*, 2016 Executive Order (EO) 13747 on *Advancing the Global Health Security Agenda To Achieve a World Safe and Secure From Infectious Disease Threats*, 2019 EO 13887 on *Modernizing Influenza Vaccines in the United States, and the HHS Strategic Plan*, OGA will support global, multilateral, bilateral, and inter-and intra-government initiatives and bring its technical, policy, and diplomatic expertise to promote policies that include:

- Enhancing local, national, regional, and global influenza preparedness and response efforts for seasonal influenza, and pathogens of epidemic or pandemic potential, including by supporting the implementation of the WHO Global Influenza Strategy 2019-2030
- Providing core subject matter expertise to develop USG policy and support negotiations around the WHO Pandemic Accord
- Strengthening other nations' commitments to fulfill their obligations under the Pandemic Influenza Preparedness (PIP) Framework
- Enhancing influenza and respiratory disease surveillance, through WHO and partner nations, including by taking steps to eliminate or mitigate delays and disruptions to rapid, systematic, and timely international influenza virus sharing, including seasonal viruses, sharing of genetic sequence data on publicly accessible platforms
- Promoting linkages between influenza capabilities and national influenza preparedness and response plans, together with broader IHR and immunization implementation efforts
- Strengthening of Emerging Infectious Diseases networks to improve risk-communication and promote vaccine confidence and trust to enhance seasonal influenza vaccination
- Identifying gaps in and priorities for sustainable, scalable global influenza vaccine production, supply chains, and distribution networks and to promote sustainability of influenza vaccine manufacturing and pandemic supply chain in developing countries in line with the 2019 Influenza vaccine modernization (EO 13887) and the 2022 Bioeconomy (EO 14801) Executive Orders
- Coordinating relevant Global Health Security Agenda (GHSA), Global Health Security Initiative (GHSI), North American Plan for Animal and Pandemic Influenza (NAPAPI)-related activities, including those focused on pandemic influenza and other biological threats
- Continuing to lead the U.S. IHR National Focal Point (NFP) to facilitate domestic implementation of the IHR and work with WHO and other countries' NFPs to strengthen compliance with IHR requirements to build public health capacities to detect, assess, report, and respond to potential public health emergencies of international concern.

OGA Pandemic Negotiator

The 2024 Budget includes $1,000,000 to fund OGA's work on the proposed new instrument on pandemic prevention, preparedness and response which will be negotiated under the constitutional authority of the World Health Organization (WHO). This funding will support the work of the Intergovernmental Negotiating Body (INB) tasked by the World Health Assembly with development and negotiation of the new instrument. These resources will allow OGA to enhance international outreach and coordination, taking lessons-learned from COVID-19 to better prepare for seasonal influenza epidemics and outbreaks of other pathogens with pandemic potential. OGA will focus on enhancing vaccine development, manufacturing, and delivery efforts; strengthening global supply chain systems; and strengthening the global architecture, including sustainable financing and accountability for global health security capacity

building efforts globally. This funding will enhance OGA's ability to ensure HHS equities, including those of its Operating Divisions, are reflected in the outcomes of the new instrument negotiations.

Five Year Funding Table

Fiscal Year	Amount
FY 2020	7,009,000
FY 2021	7,009,000
FY 2022 Final	7,009,000
FY 2023 Enacted	7,009,000
FY 2024 President's Budget	8,009,000

Program Accomplishments

The accomplishments from the HHS/Office of the Secretary International Pandemic Influenza funds have substantially advanced USG global health security priorities in countries that are critical to advancing U.S. foreign policy goals and support to HHS programs preparing for seasonal influenza epidemics or the next influenza pandemic or other pandemic threat.

Significant Accomplishments include:

Worked with WHO and international partners to strengthen and maintain the functioning of the PIP Framework, including around its possible interface with the WHO Member State negotiations around a future pandemic instrument, to ensure continued rapid and timely sharing of influenza viruses of pandemic potential

- Supported the White House National Security Council (NSC) by coordinating interagency discussions and development of a strategy to promote rapid sample sharing of influenza viruses with the Government of the People's Republic of China
- Supported WHO efforts to strengthen the Global Influenza Surveillance and Response System (GISRS), including leveraging the strong foundation of influenza surveillance to integrate surveillance of other respiratory disease threats, such as SARS-CoV-2
- Supported initiatives to improve sustainability of developing countries improving surveillance, detection, and response for influenza, and other emerging infectious disease (EID) threats affecting their countries and regions, including efforts to expand sustainable local and regional medical countermeasure manufacturing capacity
- Prioritized influenza pandemic preparedness and promoted vaccine confidence through ministerial-level side events at the World Health Assembly
- Supported the development of forecasting and budgeting tools for influenza vaccinations for low- and middle-income countries through the Task Force for Global Health and Ready2Respond
- Led the global discussion to promote rapid, systematic, and timely international influenza virus sharing, including seasonal influenza viruses
- Led U.S. engagement in the GHSI (G7 countries, Mexico, the European Commission, and WHO) to coordinate international preparedness efforts to address pandemic influenza, emerging infectious diseases with pandemic potential, and Chemical, Biological, Radiological, and Nuclear (CBRN) threats, and COVID-19 response activities

- Led U.S. engagement in the GHSA, including across the various groups (e.g., Steering Group, Action Package Working Groups, Task Forces, and led the creation of GHSA Action Packages on Sustainable Financing and Legal Preparedness)
- Supported the Pan American Health Organization (PAHO) influenza team to ensure that the lessons learned, and capacities built during the regional response to COVID-19 are used to strengthen regional preparedness efforts for influenza and other respiratory diseases
- Led the trilateral and multi-sectoral NAPAPI Health Security Working Group as the Co-Chair and Secretariat to promote greater cross-border health security in the region
- Led policy coordination for key global health security international treaties, agreements, and arrangements addressing challenges related to the implementation of the PIP-FW and the implications of the Nagoya Protocol to pathogen sample and genetic sequence data sharing.
- Led implementation of IHR NFP activities in the U.S.

Assistant Secretary for Administration

Cybersecurity

Budget Summary
(Dollars in Millions)

	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2024 +/- FY 2023
HHS Cybersecurity Program	**71.415**	**100.00**	**188.326**	**88.326**
FTE	**110**	**143**	**143**	**--**

Allocation Method .... Direct Federal

Program Overview, Cybersecurity Challenges, Requirements, and Priorities

Program Overview: The Healthcare and Public Health (HPH) sector continues to be a primary target for some of the most advanced cybercriminals in the world. As a matter of national security, the HHS Cybersecurity program requires the requested levels in support of the challenges that accompany rapidly changing technologies and the influences of hostile actors.

The cybersecurity threat landscape continues to evolve at a rapid pace with a heightened focus on the HPH sector as a prime target for bad actors. The unprecedented volume of threat activity in the sector over the last several years, the COVID-19 pandemic, and high-profile global cybersecurity events pose significant challenges to the HHS Cybersecurity program mission. These activities demonstrate cybersecurity vulnerabilities have the potential to dramatically impact the critically necessary HHS mission and the HPH sector.

The HHS Cybersecurity program, within the Office of the Chief Information Officer (OCIO), under the Assistant Secretary for Administration (ASA), assures that all information systems throughout HHS are designed, operated, and maintained with the appropriate information technology security and privacy data protections. HHS continues to increase its protections against cyberthreats, which pose great risk to HHS' critical functions and services, in addition to the confidentiality, integrity, and availability of HHS data. These threats include unauthorized access and exfiltration of sensitive data, denial of service, malicious code, inappropriate usage of HHS information and information systems, and insider threats.

Cybersecurity Challenges: Cybersecurity, privacy, and end-of-life legacy systems remain the top three IT challenges facing HHS. As the capabilities of bad actors evolve and expand - specifically increased sophistication in phishing, malware, and ransomware campaigns – so must HHS capabilities to detect and respond to those threats. The HHS cyber program must also be proactive, responsive, and able to stay ahead of adversarial innovation. To do this, HHS must be able to invest in tools, technologies and talent that provides focus on timely and proactive detection of previously unseen approaches by malicious actors.

Cybersecurity Requirements: The HHS Cybersecurity program and its many functions are mandated, in whole or in part, by increasing federal mandates, many of which also impact the HPH sector and HHS' role in the sector. The number of mandates exceeds over 100 including notable Executive Orders such as EO 14017 - *America's Supply Chains,* EO 14028 - *Improving the Nation's Cybersecurity,* and EO 14034 - *Protecting Americans' Sensitive Data from Foreign Adversaries.* These Executive Orders cover a broad range of activities. HHS is focused on three cybersecurity requirements:

1. Modernizing federal HHS cybersecurity

2. Improving the detection of cybersecurity vulnerabilities and incidents on HHS networks
3. Improving HHS investigative and remediation capabilities.

Cybersecurity Priorities: Executive Order 14028 calls for the Federal government to improve its efforts to identify, deter, protect against, detect, and respond to cyber threats and actors. To accomplish the requirements under these directives, HHS has the following Cybersecurity priorities:

1. **PRIORITY ONE:** Implementation of a Zero Trust architecture throughout the HHS environment.
2. **PRIORITY TWO:** Improving the adoption of multifactor authentication (MFA) and encryption.
3. **PRIORITY THREE:** Enhancing logging and remediation.
4. **PRIORITY FOUR:** Continuing the deployment of previously identified capabilities across HHS, such as the capabilities provided under the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program for inventory, Endpoint Detection and Response (EDR), MFA and encryption.
5. **PRIORITY FIVE** – Expand HPH sector support by maturing established programs such as the HHS Health Sector Cybersecurity Coordination Center (HC3), the Cybersecurity Act of 2015 (CSA) program, and Section 405(d) programs (405d), while establishing an HPH sector cybersecurity incident management capability. Incident management, HC3 and 405d programs strengthen the cybersecurity posture of the healthcare and public health sector.

HHS Cybersecurity Program Description and Accomplishments

The HHS Cybersecurity program implements a comprehensive, enterprise-wide program to protect the critical information with which the Department is entrusted. HHS continually increases its protections against cyber threats, such as unauthorized access, denial of service, malicious code, inappropriate usage, and insider threat, all of which pose risks to HHS critical functions, services, and data. HHS already has achieved significant maturity in identity management and automation and has made large improvements in multi-factor authentication for both citizen-facing and internal services.

Currently the program oversees approximately 800 systems, 381,000 endpoints, and 63 high value assets. The program identifies and oversees the disposition of nearly 8,000 managed cyber incidents. The program maintains an internal ethical phishing program demonstrating 96% of the total phishing exercises result in user detection and avoidance. The phishing exercise demonstrates users are gaining the ability to spot attempts to infiltrate HHS systems. Additionally, through the program, HHS Healthy Technology program trains thousands of HHS users throughout the year. The program's cyber-focused on-demand resources, called CyberCARE, saw 73,000 website views this year. The HHS cybersecurity program conducted over 3,000 web application web vulnerability scans resulting in the scanning of nearly a million web pages. Approximately 260,000 vulnerabilities were prevented from being exploited.

The program partners with over 25 Federal groups including the National Security Agency (NSA) and the Department of Homeland Security (DHS) to improve the Department's cybersecurity posture in real time. The Cybersecurity program has streamlined collaboration during cyber events across the Department and established relationships with both the public and private health sectors. The program continues to lean forward; the integration of cybersecurity in the Department's overarching Enterprise Risk Management (ERM) program has led to HHS being regarded as a risk management thought leader.

The program continues to bolster the healthcare sector's cybersecurity posture. The HHS 405(d) Program, though the HHS HC3, routinely creates HPH focused cybersecurity awareness materials that are utilized in any size organization. The program has released more than 80 cybersecurity awareness

resources which organizations across the HPH sector leverage to implement best practices and raise cybersecurity awareness within their organizations. Twenty-five of these resources were released in the first half of 2022 alone. This public-private partnership program has become one of the leading HPH focused cybersecurity platforms with an average of 80,000 visits per month to the 405(d) public website and over 2,000 subscribers representing a cross-section of entities in the HPH sector.

HHS has consistently demonstrated the ability to protect its networks, data and systems while providing much-needed support and guidance to the HPH sector. Investments is needed now to ensure these initiatives can continue and can be scaled to meet the continually evolving threat landscape.

Cybersecurity Program Capabilities: The HHS comprehensive, enterprise-wide Cybersecurity program can be grouped as a tactical delivery of cybersecurity capabilities and a more strategic information security modernization program. These cybersecurity capabilities and services include:

- Cybersecurity Operations and Engagements
- Cybersecurity Risk, Governance, FISMA Compliance, and Privacy Management
- Cybersecurity Technologies, Innovations, and Enterprise Solutions

Funding History

Fiscal Year	Amount
FY 2020	$57,820,000
FY 2021	$57,820,000
FY 2022	$71,415,000
FY 2023	$100,000,000
FY 2024 President's Budget	$188,326,000

Budget Request

The FY 2024 request for the HHS Cybersecurity program is $188,326,000, which is an increase of $88,326,000 compared to FY 2023 Enacted. The FY 2024 request will allow HHS to manage existing solutions, address cybersecurity mandates through targeted initiatives, and complement current network protection tools. The requested funds continue support the sustainment of the Department's existing cybersecurity and privacy programs while also enabling deployment of cybersecurity initiatives aligned to the HHS priorities. In addition to the existing and emerging priorities supported by the cybersecurity program, requested funding provides support for the implementation of Zero Trust, improvement of MFA and encryption, improved logging, and expanding support of the HPH sector. These activities are mandated by Executive Orders, OMB memoranda and law.

Funding at the requested level reinforces the program's capability to ensure technologies, programs, and people achieve HHS objectives, protect information, and facilitate compliance with federal mandates and guidelines. In addition to these activities, HHS is responsible for implementing the requirements of EO 14208, a key cybersecurity driver. Other key cybersecurity mandates include:

- Coordinating and supporting the deployment of Zero Trust architectures across HHS operating environments, including on-premise and cloud platforms, and
- Enhancing data logging, event correlation, endpoint detection and incident response including implementing a consolidated enterprise security and network operations capability.

Cybersecurity Funding Alignment: Changes in cybersecurity priorities and response drive funding levels. The FY 2024 Budget reinforces HHS' ability to provide vulnerability response while putting in place greater more proactive cybersecurity protections more quickly and effectively. Lack of funds at the requested level puts these efforts at risk. The FY 2024 Budget request directly aligns the HHS Cybersecurity Priorities and ensures ongoing continuation for:

- Enhancing HHS' cybersecurity strategy to meet the evolving threat landscape and sophistication of attackers. HHS' protections, tools, technologies, and talent must evolve, or HHS information and networks will be compromised.
- Engaging and expanding HPH sector-wide collaboration and information sharing. HHS has a responsibility to its components and the sector to cultivate partnerships and share information. Lack of continuous information sharing may result in the HHS or its sector partners facing significant threats and vulnerabilities for which they are unprepared.

The FY 2024 Budget request also enhances:

- Support for the implementation of a Zero-Trust architecture
- Expanding identity and access management tools and services
- Executing Zero-Trust policy-based access
- Modernizing the enterprise network to enable Zero-Trust principles, capabilities, competencies (maintaining, enhancing, and deploying tools and technologies that enable us to stay ahead of our attackers).

Program Initiatives: Requested funding will also enable deployment of cybersecurity initiatives aligned to the expanding threat environment, legislative mandates, and Presidential directives. Program initiatives supporting the HHS cybersecurity priorities include:

- Establishing a zero-trust architecture and strategy requiring HHS components to meet specific cybersecurity standards and objectives.
- Reinforcing the Department's defenses against increasingly sophisticated and persistent threat campaigns. Improve predictive, investigative, and remediation capabilities related to cybersecurity events. Strengthen the ability to predict and respond to incidents when and even before they occur.
- Prioritizing recruitment, capture, maturing, and retaining an effective cybersecurity federal workforce. HHS must invest in expanding cybersecurity technologies, but it must also ensure an evolving remote cyber workforce to stay ahead of challenges.
- Improving information sharing between Public and Private sectors and encourage healthcare to augment and align investments with the goal of minimizing vulnerabilities and future incidents

Significant funding levels are required to maintain existing cybersecurity capabilities, execute initiatives supporting HHS cybersecurity priorities, and implementation of the requirements under EO 14028 (and associated directives).

Summary of Cybersecurity FY 2022-2024
Funding by National Institute of Standards and Technology (NIST) Cybersecurity Framework
(Dollars in Thousands)

NIST Framework	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2023 +/- FY 2024
Cyber Human Capital (Non-add)	$19,772	$22,039	$26,606	$4,567
Sector Risk Management Agency (SRMA) (Non-add)	$5,636	$4,525	$4,525	--
Zero Trust Implementation (Non-add)	--	$7,887	$50,818	$42,931
PROTECT	$20,652	$30,190	$64,673	$34,483
DETECT	$16,880	$26,213	$68,375	$42,162
IDENTIFY	$27,423	$33,252	$40,390	$7,137
RESPOND	$3,769	$6,466	$10,776	$4,310
RECOVER	$2,692	$3,878	$4,112	$234
Total Cyber Request	**$104.435 /1**	**$100,000**	**$188,326**	**$88,326**

/1 $71.4 million was appropriated for Cyber in FY 2022. $104.4 million reached by including $33 million in COVID-19 supplemental resources.

Summary of Cybersecurity FY 2022-2024
Funding by Activity
(Dollars in Thousands)

Cybersecurity Activities and Initiatives	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2023 +/- FY 2024
Cybersecurity Operations and Engagement Activity	$11,560	$21,387	$21,892	$505
Cybersecurity Risk, Governance, FISMA Compliance, and Privacy Management Activity	$30,720	$34,787	$38,459	$3,672
Cybersecurity Tools and Enterprise Solution Activity	$29,130	$32,644	$44,525	$11,881
Zero-Trust and Cybersecurity Supply Chain Risk Management Initiative	$0	$7,887	$50,818	$42,931
Security Event Logging Initiative	$0	$3,295	$32,632	$29,337
Total	**$71,415**	**$100,000**	**$188,326**	**$88,326**

HHS Cybersecurity Program Enterprise Activities

Cybersecurity Programs: As part of its total funding cyber funding request, the HHS Cybersecurity Program performs many activities to ensure cybersecurity across the HHS enterprise. The program provides cybersecurity operations and engagement activities which include engagement with the HPH sector, cyber threat hunting, intelligence, and awareness including cybersecurity situational awareness functions. The program also executes cybersecurity risk management, governance, Federal Information Security Modernization Act (FISMA) compliance, and privacy management functions across the Department. These programs also provide for cybersecurity solutions, systems, and resources in support of and leveraged by the Department.

Cybersecurity Initiatives: The Department must invest in compliance with federal directives, mandates, and legislation and respond to a quickly evolving threat environment. Funding from this request also supports maturing and increasing cybersecurity tools and enterprise cybersecurity solutions Department-wide. These tools and solutions include licenses, security infrastructure, software, and next generation security technologies (including solutions addressing, cloud logging, encryption, enterprise malware, content filtering, data loss prevention, vulnerability-scanning, automated reporting, logging, analysis, and security weakness tracking).

Program and Initiative Funding Totals: Total funding for programs and initiatives results in a total increase of $88,326,000 compared to FY 2023 Enacted. Increased funding synergistically with more targeted execution of program funding is necessary to respond to both increasing legislation, mandates, and directives, and an evolving cyber threat landscape. Coupled with the rapid proliferation of information assets, the increased mobility of the HHS workforce, and the need to derive value and intelligence from information assets, these actions collectively have forced HHS to redefine its approach to managing and protecting information assets. An investment in programs and initiatives such as Zero Trust and security logging is a response to the most current threat environment, mandates, legislation, and Presidential Directives. Alignment of funds is detailed by the Program's activities and cybersecurity initiatives as follows:

Cybersecurity Operations and Engagement (CSO) Activities ($21,892,000): The request is an increase of $505,000 compared to FY 2023 Enacted. Funding accounts for stronger program activity and supports enhancement and expansion of proactive cyber hunting, threat intelligence, and risk qualification capabilities to improve the Department's cybersecurity situational awareness.

CSO has coordinated response across the Department and **Healthcare and Public Health (HPH) Sector**. As the number of cybersecurity incidents in the healthcare industry continue to increase, HHS must establish a stronger ability to support the HPH sector when incidents occur. Funding will strengthen the existing HPH sector support and establish an enhanced incident management team that can better:

- Track incidents when they occur
- Reach out to targets of these attacks to offer support
- Document and communicate the nature of the attacks to enhance threat warnings to others.

CSO capabilities are deployed to proactively prevent attacks or, in the event of a successful attack on the enterprise, minimize the impacts. CSO addresses many threat vectors simultaneously by having a central view into all Department networks. As threats evolve and become more sophisticated and technology changes, attention to consolidated data automation, proactive threat hunting capabilities, and machine learning (artificial intelligence) will enable the Department to evolve and keep pace with those threats.

The FY 2024 President's Budget provides for security capabilities impacting both the public and private health sectors. Funding as requested strengthens and enables CSO to expand and mature tracking, event research and analysis, qualify and quantify threats, resolve incidents, protect, and defend the Department's network perimeter. Requested funding provides collaboration of the cybersecurity environment with government and industry partners and stakeholders:

- **HHS and its component organizations:** Managing cybersecurity engagements and response within the Department through the CSIRC and advanced cyber defense capabilities. Funding will be applied to workforce and advanced cybersecurity support services targeted at identification, verification, and research of cyber events and incidents enhancing comprehensive mitigation strategies within the Department. Funding alignment balances more expansive, flexible, and focused data sharing and cybersecurity rigor.
- **Public sector:** Collaboration with HHS' federal healthcare delivery partners at the Department of Veterans Affairs (VA) and the Defense Health Agency (DHA) through HHS' Health Threat Operations Center (HTOC) enables advancement of Federal cyber threat predictive analytics, information sharing and engagement.
- **Private sector:** Funding will be applied to maturing cybersecurity communications and engagements with the HPH sector through the Health Sector Cybersecurity Coordination Center (HC3), enhancing the ability to respond to incidents within the private sector as necessary while providing sector entities with vital cybersecurity intelligence.

Cybersecurity Risk, Governance, FISMA Compliance, and Privacy Management Activities ($38,459,000): The request is an increase of $3,672,000 compared to FY 2023 Enacted. These necessary costs account for current cyber mission needs more effectively.

Funding for this activity aligns with continuation and advancement of cybersecurity governance, risk management, compliance, and privacy across the Department. Requested funds ensure an effective and expanding federal cybersecurity workforce and cybersecurity support services. A mature cybersecurity workforce – equipped with the appropriate training, education, and skill sets – is vital to managing the evolving threats to these information assets and adequately implementing the controls necessary for protecting HHS' information assets.

As cyber threats continue to multiply and become more complex, the need for enhanced controls and threat management strategies continues to grow. Funds advance the remediation of information security weaknesses in response to regular testing as well as findings resulting from audits conducted by the HHS Office of Inspector General (OIG) and the Government Accountability Office (GAO). In addition, funding supports expanded risk management activities as cybersecurity is integrated into HHS' enterprise risk management framework.

Funding at the requested level supports focus to the program's security compliance and annual FISMA program review efforts to effectively measure the Department and OpDiv/StaffDiv levels of compliance with FISMA requirements. Capabilities include:

- **Information security governance:** The focal point for the communication of mandatory cybersecurity requirements throughout the Department. Funding ensures information and IT assets are appropriately secured and compliant with federal regulations and best practices, to include adherence with FISMA and the Federal Information Technology Acquisition Reform Act (FITARA).
- **Information security risk management:** Department-wide evaluation of vulnerabilities and threats to HHS enhancing more effective risk-based decision making. Advancements to this

capability ensures cybersecurity's integration into HHS' Enterprise Risk Management framework, analysis of HHS high value assets, the deployment of DHS' CDM program, and adherence to the Federal Risk and Authorization Management Program (FedRAMP). Advancements strengthen review and authorization of cloud-based technologies enabling HHS to meet its mission with more cost-effective, scalable solutions.

- **Information security compliance:** Management of FISMA-focused reporting, cybersecurity audits, and oversight initiatives for the Department. Funds assure accurate interpretation of requirements, documentation of information, status of IT systems and related information, and DHS and OMB reporting. These reviews and reports strengthen and mature oversight of information security across the Department.
- **Office of the Secretary security services:** Funding directly supports publishing of information security policies while executing risk management, compliance, and security operations for the Office of the Secretary (OS) and OS Staff Divisions.
- **Privacy services:** Funding support scaling and maturation for compliance with Department policy and standards, including quarterly evaluation of security weakness Plans of Action and Milestones (POA&M), Privacy Impact Assessments (PIA), and system of records notice (SORN) compliance. Support expands activities of the HHS PII Breach Response Team to enable the Department's evaluation of OpDiv and StaffDiv breach response assessments. provides privacy governance and advisory support, reduces exposure to privacy risks, mitigates privacy risks, develops privacy policy. Services include the review and approval of all Privacy Impact Assessments (PIAs), coordinating breach response activities, and FISMA privacy reporting.
- **Aligning healthcare industry security approaches:** Funding aims to raise cybersecurity awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. The Cybersecurity Act of 2015, Section 405(d) is addressed through the 405(d) Program as a collaborative effort between industry and the federal government and cooperatively engages alongside the HC3.

Cybersecurity Tools and Enterprise Solution Activities ($44,525,000): The request is an increase of $11,881,000 compared to FY 2023 Enacted. Funding accounts for continued operations of a heightened security framework, maturing the current framework, and investment in cybersecurity solutions responding to current mandates and the threat landscape. Funding supports maturing and increasing Department-wide licenses, security infrastructure, software, and next generation security technologies. Key systems for tools innovation and investment include:

- Innovating technology and building cybersecurity resources to improve efficiencies in machine learning and automation including automated discovery and a complete inventory of Department assets connected to the internet. Utilizing innovations to meet HHS objectives to protect its mission and information. Funding addresses improvements in real time visibility of network events.
- Advancing risk management solutions to enable HHS' correlation of cyber threat and vulnerability information. Funding also enables cyber risk quantification and drives cost efficiencies through automation of governance processes.
- Increasing situational awareness and response to actions that could exploit or jeopardize HHS information systems. This investment also enables cyber risk quantification, security coordination, orchestration, automation, and response.

- Leveraging crowdsourced partnerships with AI and machine learning solutions to scan, test, and analyze assets searching for and reporting of vulnerabilities and threat opportunities.
- Threat intelligence solutions and tools providing malware intelligence, credential intelligence, vulnerability, and adversary intelligence.
- Refining HHS' network protection through deception solutions, intrusion detection, and threat response to better manage and prevent future attacks.

Zero-Trust and Cybersecurity Supply Chain Risk Management Initiative ($50,818,000.00): The request is an increase of $42,931,000 compared to FY 2023 Enacted. Funding more effectively responds to EO 14208.
In addition to the cybersecurity focused EO 14028, the Office of Management and Budget (OMB) issued additional requirements under the directives M-21-31, "*Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*" and M-22-09, "*Federal Zero Trust Strategy*." The requested levels are necessary to fund implementation of Zero Trust and associated requirements, per HHS Priority One. With these funds, HHS intends to enable better prevention, detection, assessment, and remediation of cybersecurity threats by coordinating and supporting the deployment of Zero Trust architectures across HHS operating environments, including on-premise and cloud platforms.

Funding allows HHS to implement smart automation more effectively protecting data based on risk levels and principles of least privilege access. Specific initiatives from this request include:

- Supporting the development of a Zero Trust architecture, which will be integrated into a selection of tools for next generation secure cloud implementation.
- Modernizing the enterprise network to enable Zero Trust principles and capabilities while improving cybersecurity supply chain capabilities and competencies.
- Expanding identity and access management tools and services to enable Zero Trust policy-based access.
- Reprioritizing workforce and cybersecurity support services to implement supply chain risk management, endpoint detection and response, insider threat, and counterintelligence.
- Specific implementation requirements at the HHS OpDiv level are not covered in this budgetary submittal and are addressed through the appropriate OpDiv Congressional Justifications.

Resources required to support the implementation of Zero Trust, as mandated by the EO, cannot be avoided. Without baseline funding increases from Congress, full implementation of the EO and OMB Directives will not be possible and will leave HHS with diminished capacity to prevent and respond to hostile cyber activities.

Smartphones, mobile, Virtual Private Networks (VPN), and cloud computing significantly changed the way the HHS stores, accesses, and secures data while meeting the protection and accessibility demanded by the public's interest. Funding enables prevention, detection, assessment, and remediation of cybersecurity threats by coordinating and supporting the deployment of Zero Trust strategy and architectures across the Department, including on-premise and cloud platforms.

Funding directly addresses systems and services to implement EO 14028, specifically focusing on Zero Trust architecture across the Department and compliance within OS. This activity includes specific resources to coordinate a Cybersecurity Supply Chain Risk Management (SCRM) program and ensure its integration into HHS' overarching supply chain risk management capabilities.

Funding addresses resources to develop an active and ongoing assessment of the Department's core architecture required to implement Zero Trust architectures. Implementation requires significant investment to prioritize use cases and redesign networks. The request enables the program to apply a granular analysis of the context, device, and user identity to strictly enforce least-privilege authorizations for each access request.

Security Event Logging Initiative ($32,632,000.00): The request includes an increase of $29,337,000 compared to FY 2023 Enacted. Increased funding accounts for supporting the current cyber mission needs while ensuring that HHS is responsive to the requirements of the EO and M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. Lack of requested funds brings increased risk to the Department's effectiveness for threat intelligence, behavior profiling and analytics, and limits the capabilities for a comprehensive, unified security event logging initiative causing HHS to fall short of full implementation of a federal requirement.

Multiple initiatives regarding EO14028 and associated memorandums including enhanced logging, endpoint detection and response, and Zero Trust architecture (e.g., M-21-31, M-22-01, and M-22-09) have dramatically elevated the need for expanded Security Incident and Event Monitoring (SIEM) log collection capabilities and centralized visibility throughout HHS. Executive Order 14028, directs "*…decisive action to improve the Federal Government's investigative and remediation capabilities."* Specifically, section 8 of the EO addresses "*logging, log retention, and log management*." Funding dedicated to expanding HHS enterprise ability to capture, store, share, and apply automated correlation activities is essential. Funds aligned for FY 2024 supplement current activity with increases and advancements across the Department.

The Security Event Logging initiative (HHS Priority Three) includes additional threat intelligence, threat logging, threat analysis, and threat response across the entire Department. The initiative enables security event logging strategies to leverage cloud service providers, increase the volume of telemetry data collected, and accelerated aggregation and correlation of logs. Aligned funding supports the ability to manage logs with updated storage capabilities and expanded retention periods. This also accelerates compliance expanding current initiatives while providing flexibility to leverage both old and new data in respond to cyber threats. Security Event Logging Initiative strengthens:

- Collection and storage of data from multiple sources in multiple formats and developing automation to enrich threat intelligence.
- Correlating more expansive data across the Department increasing the ability to isolate threat vectors.
- Categorizing data to help perform threat analytics, better recognize tactics, techniques, procedures, and correlating relationships through modeling and visualizations.
- Automate updates to threat information and risk mitigations, integrating intelligence workflow processes to further enrich and communicate findings from existing data.
- Supporting various integrations via Application Program Interfaces (APIs), bidirectional feeds, and email notifications; and supporting the sharing of intelligence across the Department and trusted communities.

Without these funds HHS has increased risk to the ability to respond and comply with increasing mandates and threats. Additionally, the Department's effectiveness for threat intelligence, behavior profiling and analytics limits the capabilities for a comprehensive, unified security event logging initiative. Limitations include:

- Continued manual reliance on human driven updates to threat information and risk mitigations as opposed to efficiencies from automated data analysis.

- Lack of real-time detection and lack of agility through visual reviews of limited data.
- Aging assets and technology not in tune with ever-evolving threats.
- Obstacles and potential inability to meet federally mandated expectations and the Administration's aggressive approach to cyber protection
- Inability to ensure Department-wide understanding of threats in real-time. Continued reliance on outdated analysis capabilities combined with outdated communication and alert processes.

The Budget request proposes a Department-wide service to collect and transmit centralized cloud log in conjunction with a Security and Network Operations Capability (SNOC). This capability consolidates network performance and traffic telemetry along with cybersecurity event and incident data enabling better visibility and reporting across the Department. The content provided by SNOC will improve awareness and decision making across HHS and depict network and security status and readiness at near real time. Funding will directly address the EO's expectation *"…ensuring centralized access and visibility for the highest-level enterprise security operations center (SOC) of each agency."*

Funding supports ensuring centralized access and visibility through consolidated security operations and network monitoring capabilities. National Cybersecurity Protection System (NCPS) compliance requirements also exist for cloud log collection and reporting to the Cybersecurity and Infrastructure Security Agency's (CISA) Cloud Log Aggregation Warehouse (CLAW).

HHS Cybersecurity - Outputs and Outcomes Table

The HHS Cybersecurity Program transitioned to new measures during FY 2022. Legacy measurements reported in prior years, and required under quarterly and annual FISMA reporting requirements, were rescinded by OMB and DHS in FY22 and are no longer tracked or collected. New program measures (outputs and outcomes) better capture and reflect federal cybersecurity priorities, including requirements mandated by EO 14028. The Program outputs and outcomes are listed below.

FY24 New Program/Measure	Most Recent Result (FY 2022 Annual)	FY 2023 Target	FY 2024 Target	FY 2024 Target +/- FY2023
System Authority to Operate (ATO): FY22 CIO Metrics and NIST 800-53: Total Number of Operating Systems: (CIO FISMA 1.1)	791	NA	NA	NA
System Authority to Operate (ATO): FY22 CIO Metrics and NIST 800-53: Total Number of Operating Systems	98.50%	95%	98%	+3%
System Multifactor Authentication: (CIO FISMA 2.3) How many [what percentage] of the systems (from 1.1.1 and 1.1.2) have mandatory PIV access enforced (not optional) for internal users as a required authentication mechanism?	67.00%	Total 100%	Total 100%	Maintain
(CIO FISMA 2.4) **Of the systems that do not enforce PIV authentication for internal users** (total number of systems from 1.1.1 and 1.1.2 less 2.3), **how many** [percentage] **enforce** (not optional) **an MFA credential that is verifier impersonation-resistant** (e.g., mutual TLS, or Web Authentication) **as a required authentication mechanism?**	37.16%	Total 100%	Total 100%	Maintain
System Multifactor Authentication: (CIO FISMA 2.5) **How many** [percentage] **systems** (from 1.1.1 and 1.1.2 less 2.3 and 2.4) **use MFA credentials susceptible to impersonation** (e.g., push notifications, OTP, or use of SMS or voice) **as the primary required authentication mechanism?**	29.88%	Total 100%	Total 100%	Maintain

Immediate Office of the Secretary

Office of National Security

Budget Summary
(Dollars in millions)

	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2024+/- FY 2023
Budget Authority	**8.510**	**8.983**	**11.983**	**+3.000**
FTE	**38**	**38**	**56**	**+18**

Allocation Method .... Direct Federal

Program Description and Accomplishments

The Office of National Security (ONS) was established in 2007 and in 2012 was designated by the Secretary of Health and Human Services (HHS) and the Director of National Intelligence (DNI) as the Department's Federal Intelligence Coordination Office (FICO). In this capacity, ONS is the HHS point of contact with the Intelligence Community (IC) and is responsible for coordination with the IC and for intelligence and national security support to the Secretary, senior policy makers and consumers of intelligence across the Department. Additionally, ONS is responsible for safeguarding classified national security information across the Department and the appropriate sharing of intelligence, homeland security and law enforcement information externally and internally within HHS among the Operating and Staff Divisions. ONS is headed by the Director, who reports directly to the HHS Deputy Secretary. The Director serves as the HHS Secretary's Senior Intelligence Official on national security, intelligence and counterintelligence issues, the Senior Designated Official for insider threat issues, and as the Department's Federal Senior Intelligence Coordinator (FSIC). The Director has also been delegated original classification authority by the Secretary.

Besides the Immediate Office of the Director, ONS is comprised of five divisions, including the Intelligence and Analysis Division (IAD), the Staffing and Business Services Division (SBSD), the Personnel Security (PerSec) Division, the Operations Division, and the Enterprise Supply Chain Risk Management Division. These divisions are responsible for integrating intelligence and security information into HHS policy and operational decisions; assessing, anticipating, and warning of potential security threats to the Department and our national security; and providing policy guidance on and managing the Office of the Secretary's implementation of the Department's national security, intelligence (including cyber intelligence), and defensive counterintelligence/insider threat programs. ONS divisions identifies, assesses, and mitigates the risk to the integrity, trustworthiness, and authenticity of mission-critical products, materials, information, and services within the Department's internal supply chain. Many of these come from supply chains that interface with or operate in a global marketplace. Addressing the activities of adversaries and having a greater understanding of the risks inherent to the Department's participation in the global marketplace is crucial to safeguarding the Department's mission and the nation's health and wellness.

ONS integrates and synthesizes intelligence and all-source information on public health, terrorism, national security, weapons of mass destruction and homeland security, in order to support HHS missions, enhance national security and help keep Americans safe. More specifically, ONS programs include classified national security information management, secure compartmented information facilities

management, communications security, safeguarding and sharing of classified information, cyber threat intelligence and intelligence analysis and counterintelligence/insider threat. This operational responsibility is in support of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA); Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; and other relevant Executive Orders (including Executive Order 12333), Intelligence Community Directives, Presidential Directives, and policy guidance. ONS has responsibilities to establish implementing guidance, provide oversight, and manage the Department's policy for the sharing, safeguarding, and the coordinated exchange of information related to national or homeland security with other federal departments and agencies, including law enforcement organizations and the IC, in compliance with HHS policies and applicable laws, regulations, and Executive Orders.

Operational Environment

HHS is the world leader for medical research, medical product and pharmaceutical regulation, the administrator for billions of program dollars supporting health and human services programs domestically and internationally, and the principal repository for personal medical and health related data. As such, HHS is a primary target for physical attacks as well as cyber-attacks, theft of intellectual property, technical data, or sensitive information from insider threats, and foreign intelligence services or actors.

ONS established a cadre of intelligence, counterintelligence and cyber threat intelligence analysts, and special security professionals, to acquire, synthesize, analyze, and report on open source and classified information and assess its usefulness in supporting and furthering the HHS mission. ONS utilizes all-source classified and unclassified information from the IC, as well as from Law Enforcement, Homeland Security, and other stakeholder organizations to provide a comprehensive national or homeland security assessment to HHS senior leadership and others across the Department. In addition, ONS represents HHS on a number of external committees and councils responsible for interagency coordination on security threats, intelligence, counterintelligence, insider threat and cyber threat intelligence issues, including the sharing and safeguarding of national security information.

Funding History	
Fiscal Year	**Amount**
FY 2020	8,510,000
FY 2021	8,510,000
FY 2022 Final	8,510,000
FY 2023 Enacted	8,983,000
FY 2024 President's Budget	11,983,000

Budget Request

The FY 2024 request for ONS is $11,983,000 which is a $3,000,000 increase over the FY 2023 Enacted.

ONS continues to maintain its capability to provide timely, appropriately tailored and relevant intelligence, and other strategic (including law enforcement sensitive) information to inform HHS decision-makers and their programs on potential national security threats domestically and abroad. Intelligence/Information is used by HHS to anticipate and warn of emerging threats that may require the

department to adjust policy/programs; achieve global health security goals such as those related to the Ebola Epidemic; address major cyber intelligence-related threats (especially threats directed at healthcare infrastructure); and support broader national security interests.

In addition, the continuing cyber threats to the Department's vital systems and information, and threats to the Healthcare and Public Health sector (including ransomware), make cyber threat intelligence critical to preventing and mitigating these incidents. ONS' ability to maintain and work closely with other federal departments and agencies, including law enforcement organizations and the IC, will help ensure the protection of both federal critical infrastructure and the public health and health care sector, and provide deterrence and mitigation strategies from cyber security threats. Additionally, ONS continues to maintain the Department's capability to address 1) supply chain risk management, 2) vetting of foreign national visitors, 3) assessing potential damage to HHS and national security from unauthorized disclosure of classified and/or sensitive information, and 4) addressing potential cyber threats to the Nation's public health and medical infrastructure.

The 2024 Budget includes an increase of $3 million for 18 additional FTE to enable ONS to address the increased workload and take a more proactive approach in the four programs noted below in order to better protect the Department.

Program #1 - Enterprise Supply Chain Risk Management (E-SCRM): HHS faces significant challenges in managing agency risk across its dynamic mission and its extensive array of networks and information systems. The E-SCRM Program identifies, assesses, and mitigates the risk to the integrity, trustworthiness, and authenticity of mission-critical products, materials, information, and services within the Department's internal supply chain. Many of these come from supply chains that interface with or operate in a global marketplace. Addressing the activities of adversaries and having a greater understanding of the risks inherent to the Department's participation in the global marketplace is crucial to safeguarding our Department's missions and the nation's health and wellness.

The Department's approach to meeting the requirements of statutes, Executive Orders, and regulations is an enterprise approach to managing threats and risks associated with the lifecycle (acquisition, sustainment, and disposal) of mission-critical products, materials, information, and services used throughout the Department and Divisions. This will be accomplished by establishing a Department-level E-SCRM program in ONS to oversee and coordinate E-SCRM matters. The development of a strategy and implementation plan will lay out the roadmap for implementing effective Department E-SCRM capabilities, practices, processes, and tools within the enterprise and support HHS's vision, mission, and values. This roadmap includes E-SCRM governance and coordination through policies, Cyber SCRM policies, role-based training, threats and risks analysis, and information sharing with coordinated decisions.

The HHS E-SCRM program is intended to shape policies, guidance, practices, processes, and procedures needed to implement a robust supply chain risk management capability. It is understood that E-SCRM policy at the Federal level is rapidly evolving, therefore, the E-SCRM program will be postured to adapt to the evolving policy environment.

Program #2 - Information Security Program: HHS houses a plethora of information on public health and operations that may be considered unclassified but if released could cause a detriment to the agency or the United States. The Information Security Program includes the protection of sensitive unclassified and classified information. Currently, ONS has just one part-time employee supporting the protection of sensitive unclassified information and requires additional FTEs to begin meeting National Archives and

Records Administration (NARA) requirements for the protection of Controlled Unclassified Information. The Budget includes additional FTEs to support the protection of sensitive unclassified information for the Department as required by NARA regulations.

Program #3 - Insider Threat Program: As security concerns arise in the Department, HHS ONS must further the development of a robust and effective Insider Threat Program to follow E.O. 13587. This threat mitigation program needs additional resources to be able to detect and identify improper or illegal actions, assess threats to determine levels of risk, and implement solutions to manage and mitigate the potential consequences of insider incidents across the department. ONS serves as the insider threat lead and coordinates with other offices (e.g., OIG, HR, security) through a Hub concept to ensure insider threats are properly addressed as they arise. The further development of this team will also allow for strategic case processing/tracking, more in-depth coordination with federal partners, and more analysis.

Program #4 - Cyber Threat Intelligence Program: HHS ONS, in partnership with the HHS Office of Information Security within the Office of the Chief Information Officer, is responsible for the establishment and maintenance of the Cyber Threat Analysis Program (CTAP). The CTAP serves to address risks and maintain situational awareness on national security related cyber threats to increase the overall security posture of the Department. The CTAP is responsible for the integration of forensic and analytical capabilities to address the prevalent national security related cyber threats and support the operational mission of HHS Operating Divisions (OpDivs) most targeted for their highly sought-after intellectual property, sensitive technical data, research, economic data, personal identifiable information (PII) and protected health information (PHI). As the principal agency for protecting U.S. PHI, HHS must maintain a vigilant Department-wide advanced cyber threat analytical capability to prevent, detect, respond to, and mitigate national security related threats. Cyber threats to the Department have significantly increased in recent years. Additional FTE will enable ONS to proactively focus on these threats instead of just having a reactive stance.

Assistant Secretary for Health

Commissioned Corps Readiness Training

Budget Summary
(Dollars in Millions)

Commissioned Corps Readiness Training	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2024 +/- FY 2023
Budget Authority	--	--	2.000	+2.000
FTE	--	--	2	2

Authorization Legislation ....PHS Act, Title I, Section 204 & 204a
FY 2024 Authorization .... Permanent
Allocation Method .... Direct Federal

Program Description

The Assistant Secretary for Health is the head of the USPHS Commissioned Corps (Commissioned Corps), which is one of the eight uniformed services. The Commissioned Corps includes the Regular Commissioned Corps, Ready Reserve, and Public Health Emergency Response Strike Team (PHERST). The Surgeon General oversees the day-to-day operations of the entire Commissioned Corps, and Commissioned Corps Headquarters (CCHQ) is responsible for personnel, administration, medical, training, readiness, deployment operations, and policy for both the active duty and reserve components of the Commissioned Corps.

Regular Corps officers fill clinical and service positions across more than 21 federal departments, both within the Department of Health and Human Services (HHS) (e.g., Indian Health Service, National Institutes of Health and Centers for Disease Control), as well as non-HHS agencies (e.g., Federal Bureau of Prisons (BOP), Department of Defense, and Department of Homeland Security). The PHERST is also comprised of Regular Corps officers. Ready Reserve officers serve on a part-time basis, and together with PHERST officers, provide the Department with a critical public health and readiness resource. All officers must maintain readiness to deploy and respond to public health crises, disease outbreaks, and humanitarian missions, because they deploy at the direction of the President and the Secretary during public health emergencies and national disaster declarations.

Examples of such deployments include but are not limited to national and global crises involving natural disasters, infectious disease threats, urgent public health needs, and biological security threats. In recent years, requests for deployment of Public Health Service officers expanded considerably. Deployments include critical medical and public health support such as providing medical support along the southwestern border and Operations Allies Welcome where the USPHS Commissioned Corps supported medical operations for repatriated Afghans. The USPHS Commissioned Corps deployed over two-thirds of its officers in support of COVID-19, the highest historic deployment of officers. In addition, the USPHS Commissioned Corps continues to provide public health and medical support at large scale national events including the State of the Union, Boston Marathon, and Independence Day Celebrations in Washington, D.C.

Budget Request

The FY 2024 President's Budget request for Commissioned Corps Readiness and Training is $2,000,000, which is an increase of +$2,000,000 over FY 2023 Enacted. This funding will fund two training FTEs, support and sustain three training contracts, and provide training related

travel for approximately 10 percent of the Corps. The funding will support training enhancement and development of officers to better meet the Corps' regional, national, and global public health emergency responses.

Five Year Funding Table

Fiscal Year	Amount
FY 2020	--
FY 2021	--
FY 2022	--
FY 2023 Enacted	--
FY 2024 President's Budget	$2,000,000

Program Accomplishments

The Coronavirus Aid, Relief, and Economic Security (CARES) Act included $16.7 million for readiness and training for Public Health Service officers. The funding is being utilized to ensure 25 percent of Public Health Service officers are trained in public health emergency response which includes access to training on chemical, biological, radiological, and environmental threats. CARES Act funding supports one additional training FTE to support the program.

CCHQ has developed a new USPHS Commissioned Corps training standard that includes clinical, emergency management, and leadership skills. CCHQ has developed new career development courses that target mid-grade officers to enhance leadership skills to ensure the USPHS Commissioned Corps is building public health leaders. Finally, additional training staff are working with partner organizations to develop a comprehensive catalogue of current training to enhance USPHS Commissioned Corps professional development in leadership, officership, and clinical deployment skills.

- The training and modernization contract was awarded to the University of Nebraska Medical Center to develop and deliver training focused on the safety of officers deployed to highly hazardous environments. 41 officers have received training through two Deployment –Safety Academy Field Experience courses.
- The emergency response training contract was awarded to Emory University. 913 officers received training through the Emergency Response Training course.

  The advanced leadership training was awarded to the Technical Management Services to develop leadership skills required to lead departments of highly trained personnel providing public health services to diverse population.
- The training delivery services contract was awarded to AFC Development Inc. to provide administrative and event planning activities as well as technical training support to the CCHQ Training Branch to deliver deployment events.

CARES Act funding also supports a partnership with the DoD via Innovative Readiness Training (IRT) and Military Facility Annual Training (MFAT), focused on improvement clinical deployment skills. For the IRT, teams of over 70 Public Health Service officers were embedded with DoD soldiers and officers in rural settings across the country (e.g., Alaska, Tennessee, Hawaii, Georgia and Oklahoma). For MFAT, a team of four Public Health Service officers were embedded with DoD's Tripler military treatment facility in Hawaii. These trainings are a critical component of training in engineering, occupational health, clinical care, and clinical support. As of January 25, 2023, a total of 2,899 officers have been trained with CARES Act funding.

U.S. Public Health Service Ready Reserve

Budget Summary
(Dollars in Millions)

U.S. Public Health Service Ready Reserve	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2024 +/- FY 2023
Budget Authority	-	-	13.600	+13.600
FTE	-	-	131	+131

Authorization Legislation .... CARES Act, Title III, Section 3214
FY 2024 Authorization .... Permanent
Allocation Method .... Direct Federal

Program Description

The Assistant Secretary for Health is the head of the USPHS Commissioned Corps (Commissioned Corps), which is one of the eight uniformed services. The Commissioned Corps includes the Regular Commissioned Corps, Ready Reserve, and Public Health Emergency Response Strike Team (PHERST). The Surgeon General oversees the day-to-day operations of the entire Commissioned Corps, and Commissioned Corps Headquarters (CCHQ) is responsible for personnel, administration, medical, training, readiness, deployment operations, and policy for both the active duty and reserve components of the Commissioned Corps.

Regular Corps officers fill clinical and service positions across more than 21 federal departments, both within the Department of Health and Human Services (HHS) (e.g., Indian Health Service, National Institutes of Health and Centers for Disease Control), as well as non-HHS agencies (e.g., Federal Bureau of Prisons (BOP), Department of Defense, and Department of Homeland Security). The PHERST is also comprised of Regular Corps officers.

Ready Reserve officers serve on a part-time basis, and together with PHERST officers, provide the Department with a critical public health and readiness resource. PHERST officers are a rapid deployment force located throughout the country and have broad public health expertise, including in areas such as behavioral health, social work, and public health science. Ready Reserve officers also have specific skills needed for public health emergencies (*e.g.,* ICU nurses). They sign a six-year commitment contract and are available to bolster Commissioned Corps missions.

Ready Reserve officers are paid when on active duty (including both trainings and deployments); officers are required to train (“drill’) for a minimum of 2 weekends/month (on average) and 14 days/year for annual training. In addition, Ready Reserve officers may be placed on temporary or part-time active duty to address personnel shortages at government agencies. In addition, Inactive Duty Training (IDT) allows Ready Reserve officers to maintain their skill sets monthly.

Budget Request

The FY 2024 President’s Budget Request for the Ready Reserve is $13,600,000, which is an increase of $13,600,000 above FY 2023 Enacted. At this funding level, the Ready Reserve will allow for sustaining the Reserve Corps at approximately 400 officers with 31 management FTEs. These officers will be available to bolster the Department’s public health needs and emergency response.

Five Year Funding Table

Fiscal Year	Amount
FY 2020	--
FY 2021	--
FY 2022 Final	--
FY 2023 Enacted	--
FY 2024 President's Budget	$13,600,000

Program Accomplishments

The Coronavirus Aid, Relief, and Economic Security (CARES) Act established the Ready Reserve Corps and provided the initial funding to build the infrastructure for the Ready Reserve program, recruitment, and training of its initial cohort. The USPHS Commissioned Corps has onboarded and deployed Ready Reserve officers, expanding its deployment capabilities. Thus far, the Ready Reserve team established and implemented recruitment, training, communication plans, IT infrastructure and corresponding standard operating procedures to operationalize the Ready Reserve. This includes hiring of critical personnel in CCHQ. As of February 7, 2023, the Ready Reserve has onboarded 91 officers.

Deployment Days and Mission Type		
Mission	**Officers**	**Days**
COVID (IHS)......	21	567
OAW (ACF)........	10	298
NPS.....................	1	65
RSV (IHS)...........	5	131
IRT (DoD)...........	17	149
MFAT (DoD)......	1	15
TOTAL.............	**55**	**1,325**

USPHS Ready Reserve – Key Outputs and Outcomes Table:

Measure	Year and Most Recent Result / Target for Recent Result / (Summary of Result)	FY 2023 Target	FY 2024 Target	FY 2024 Target +/- FY 2023 Target
6.1.8 Percent growth of USPHS Ready Reserve Officers Year-over-Year (or total officers).	FY 2022: 66 Target[1]: 200 (Target Not Met)	250	400	+150

[1]The FY 2022 target was established for 200 officers, however due to insufficient funding, there is a current cap at 100 officers.

Performance Analysis

The USPHS Ready Reserve continues to develop a recruitment strategy and operations plan. The framework for this new strategy consists of three key areas of focus: Communication and Stakeholder Engagement, CCHQ Infrastructure, and Performance Management. Each focus area contains a series of activities with high impact on the overall strategy as well as a detailed plan of operation. In addition, the strategy includes a performance management plan that consists of milestones, key performance indicators, and a risk management plan.

There remains a critical need for administrative and legislative support to eliminate significant barriers to recruitment, emergency and public health preparedness response, and continued support for non-emergency health care. The Ready Reserve still requires authority for dual compensation, extension of TRICARE benefits, leave rights, authority for the Secretary to call officers to active duty for training amongst others. The 2024 Budget includes legislative proposals to align Commissioned Corps' rights and benefits with those of other uniformed services. The descriptions for these proposals are included in the General Departmental Management Congressional Justification in the chapter titled "Legislative Proposals"). This coupled with the need for improvements in IT infrastructure and operations will be critical focus areas for the full implementation and continued expansion of the USPHS Commissioned Corps Ready Reserve.

Public Health and Emergency Response Strike Team

Budget Summary
(Dollars in Millions)

PHERST	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2024 +/- FY 2023
Budget Authority	**-**	**-**	**4.400**	**+4.400**
FTE	**-**	**-**	**24**	**+24**

Authorization Legislation ....PHS Act, Title I, Section 204 & 204a
FY 2024 Authorization .... Permanent
Allocation Method .... Direct Federal

Program Description

The Assistant Secretary for Health (ASH) is the head of the USPHS Commissioned Corps (Commissioned Corps), which is one of the nation's eight uniformed services. The Commissioned Corps includes the Regular Commissioned Corps, Ready Reserve, and Public Health Emergency Response Strike Team (PHERST). The Surgeon General oversees the day-to-day operations of the entire Commissioned Corps, and Commissioned Corps Headquarters (CCHQ) is responsible for personnel, administration, medical, training, readiness, deployment operations, and policy for both the active duty and reserve components of the Commissioned Corps.

Regular Corps officers fill clinical and service positions across more than 21 federal departments, both within the Department of Health and Human Services (HHS) (e.g., Indian Health Service, National Institutes of Health and Centers for Disease Control), as well as non-HHS agencies (e.g., Federal Bureau of Prisons (BOP), Department of Defense, and Department of Homeland Security). Ready Reserve officers serve on a part-time basis, called upon to serve their country when needed in underserved communities and during public health emergencies.

PHERST officers are full-time Regular Corps officers who can deploy within 8 hours, serving as "first on the ground teams." Together with Ready Reserve officers, PHERST officers provide the Department with a critical rapidly deployable public health and readiness resource. PHERST officers have broad public health expertise, and this group includes public health scientists, social workers, and behavioral health providers.

Budget Request

The FY 2024 President's Budget request for PHERST is $4,400,000, which is an increase of +4,400,000 above FY 2023 Enacted. At this funding level, the Commissioned Corps can sustain approximately 20 PHERST officers and four administrative FTEs. This funding will continue to allow the USPHS Commissioned Corps to rapidly respond to urgent, emergency public health events with highly trained professional staff.

Budget History

The Coronavirus Aid, Relief, and Economic Security (CARES) Act provided $7 million for OASH to build the initial infrastructure for the PHERST component of Commissioned Corps, including hiring and training of the first cohort. CCHQ has used this funding to develop and implement plans for recruitment, training, and communications, infrastructure and management development, and standard operating procedures for PHERST operations. As of February 7, 2023, there are 75 PHERST officers selected, and 58 officers on board readily available for deployment.

Five Year Funding Table

Fiscal Year	Amount
FY 2020	--
FY 2021	--
FY 2022 Final	--
FY 2023 Enacted	--
FY 2024 President's Budget	$4,400,000

Program Accomplishments

PHERST officers have deployed in support of numerous incidents. In September of 2021, PHERST officers responded within four hours of notification to support the Operation Allies Welcome (OAW) airport mission and continue to support other no-notice missions. They currently serve and support global USPHS trainings, such as Officer Basic Course and numerous deployments skills trainings. The following is a summary of PHERST deployments to date.

Incident Support	PHERST Deployments
COVID-19	6
Unaccompanied Children	1
Operation Allies Welcome	29
Hurricane Ian	1
Hurricane Fiona	1
Mpox Vaccine Operations	3
Ebola Screening	11

PUBLIC HEALTH EMERGENCY FUND

Budget Summary
(Dollars in Millions)

	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2024 +/- FY 2023
Budget Authority	--	--	50.000	+50.000
FTE	--	--	--	--

Authorizing Legislation:
Authorization ....Public Health Service Act, Sec. 319(b) 42 U.S.C. 247d
Authorization Status...Indefinite
Allocation Method .... Direct Federal/Intramural, Contracts, Grants

Program Description
The Public Health Service (PHS) Act created the Public Health Emergency Fund (PHEF) in 1983. The Secretary of HHS may use the PHEF to rapidly respond to the immediate needs resulting from declared or potential public health emergencies. In response to a declared or potential public health emergency, the PHS Act authorizes the Secretary to use the fund to:

- facilitate coordination among Federal, State, local, Tribal and territorial entities and public and private health care entities
- make grants, awards, and enter into contracts
- support advanced research and development of countermeasures and products, and strengthen biosurveillance and laboratory capacity
- support initial emergency operations related to preparation and deployment of intermittent disaster response personnel and the Medical Reserve Corps, and
- other actions determined appropriate and applicable by the Secretary.

Despite the Public Health Emergency Fund being authorized by the Public Health Service Act, it does not receive an annual appropriation and it has not received appropriations in decades. Congress appropriated funding to the PHEF twice – once in 1987 in response to the Acquired Immune Deficiency Syndrome epidemic, and once more in 1993 to respond to a hantavirus outbreak in the Southwest United States. The Public Health Emergency Fund is distinct from the Public Health and Social Services Emergency Fund.

Funding History	
Fiscal Year	**Amount**
FY 2020	--
FY 2021	--
FY 2022 Final	--
FY 2023 Enacted	--
FY 2024 President's Budget	$50,000,000

Budget Request

The FY 2024 budget provides $50 million for the Public Health Emergency Fund to allow the HHS Secretary to immediately respond to a public health threat or declared public health emergency, pursuant to section 319 of the Public Health Service (PHS) Act. These funds would be available until expended, consistent with the PHS Act authorization, and would allow HHS to rapidly deploy resources early in a response effort. The PHEF is a valuable tool for the government to respond rapidly to public health threats, but it has not been utilized due to a lack of available funding. Congress has frequently provided HHS with emergency supplemental funding when the need arises, including in recent years to respond to Ebola, hurricanes, and Covid-19. An annual appropriation to the PHEF would allow HHS to act without delay in response to a public health emergency, which could speed up critical public health responses while allowing Congress sufficient time to consider supplemental funding bills.

The PHEF appropriation will be held in reserve for potential use in response to any public health emergency or potential public health emergency as determined by the Secretary, consistent with section 319 of the PHS Act. These funds would complement the Infectious Diseases Rapid Response Reserve Fund (IDRRRF) authorized for use by the Centers for Disease Control and Prevention (CDC) for an infectious disease emergency if the emergency is 1) declared by the Secretary of HHS under section 319 of the PHS Act to be a public health emergency, or 2) determined by the Secretary of HHS to have the significant potential to imminently occur and potential, on occurrence, to affect national security or the health and security of U.S. citizens domestically or internationally. HHS can transfer or obligate funds from the IDRRRF to prevent, prepare for, or respond to an infectious disease emergency after notification to Congress. Funds are available to CDC and may be transferred to the National Institutes of Health and the Public Health and Social Services Emergency Fund. In contrast, PHEF would be available to respond to a public health emergency, not limited to infectious diseases, immediately upon declaration or determination of a public health emergency by the Secretary of HHS. Further, funds would be available to all HHS agencies, which would allow for a robust and tailored response to a variety of public health emergencies. Potential uses for the funding include deploying human services resources after a natural disaster, responding to the public health effects of a terrorist attack, addressing emergency nutritional needs for vulnerable populations, or responding to any other public health threat.

PANDEMIC PREPAREDNESS

Budget Summary

(Dollars in Millions)

Allocation	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2023 +/- FY 2022
Administration for Strategic Preparedness and Response	--	--	10,540	+10,540
Centers for Disease Control and Prevention	--	--	6,100	+6,100
National Institutes of Health	--	--	2,690	+2,690
Food and Drug Administration	--	--	670	+670
Mandatory Funding	**--**	**--**	**20,000**	**+20,000**

Allocation Method…………………………………………...... Direct Federal/Intramural, Contracts

Program Description

Biological threats, whether naturally occurring, accidental, or deliberate, pose serious threats for which we must be prepared. HHS's long history of leading responses to outbreaks such as H1N1, Zika, and Ebola highlights the importance of speed to saving lives—in detecting biological threats before they spread; scaling system capacity to respond to and mitigate the impact of bioincidents; and developing, securing, distributing, and communicating about tools like vaccines and therapeutics needed to prevent and lessen the impact of disease. To create the conditions for speed, effective and scalable preparedness and response systems must be put in place long before emergencies strike. The United States must catalyze advances in science, technology, and core capabilities to prepare for future biological threats.

The FY 2024 Budget includes $20 billion in mandatory funding, available over five years through the PHSSEF across the Administration for Strategic Preparedness and Response (ASPR), Centers for Disease Control and Prevention (CDC), National Institutes of Health (NIH), and Food and Drug Administration (FDA), to prepare for and respond rapidly and effectively to future pandemics and other high-consequence biological threats. Mandatory funding is requested for PHSSEF and will be allocated to these HHS agencies.

This funding will support critical priorities outlined in the 2021 *American Pandemic Preparedness Plan* and 2022 *National Biodefense Strategy and Implementation Plan for Countering Biological Threats, Enhancing Pandemic Preparedness, and Achieving Global Health Security*[2], and build on knowledge and experience gained during recent responses and prior domestic and global pandemic preparedness efforts.

This funding, alongside a suite of complementary legislative proposals, will allow HHS agencies to take critical steps to transform our nation's capabilities across the full spectrum of preparedness and response before the next pandemic hits, including by:

1. Enhancing early detection and warning systems
2. Advancing and securing safe and effective supplies and medical countermeasures; and
3. Strengthening public health systems and core capabilities.

[2] https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf

Funding History	
Fiscal Year	**Amount**
FY 2020	--
FY 2021	--
FY 2022 Final	--
FY 2023 Enacted	--
FY 2024 President's Budget	$20,000,000,000

Budget Request

The FY 2024 Budget requests $20 billion in mandatory funding, available over five years, for ASPR, CDC, NIH, and FDA. Throughout this proposal, HHS agencies invest in cross-cutting and threat-agnostic approaches that can help prepare the nation for any biological threat and bolster America's biodefense posture.

To strengthen early detection, HHS will invest through CDC to modernize detection infrastructure, improving early warning systems like wastewater surveillance and strengthening our nation's public health laboratory system. ASPR will develop threat agnostic pathogen Next Generation Sequencing (NGS)-based diagnostics for use in laboratory and remote settings—a cornerstone technology for rapid response in the 2022 National Biodefense Strategy. NIH will further strengthen early detection by supporting RADx's highly effective program to accelerate the design, validation, regulatory authorization, and manufacturing of not only laboratory tests but also point-of-care and over the counter (OTC) tests to help identify cases and inform effective treatment plans early.

To enhance the availability of tools needed to defend and protect against biological threats, HHS will invest further in basic and applied research, advanced development and licensure, and manufacturing of medical defenses. Experience has shown that investments to accelerate product development pay off—as do focused resources to accelerate their availability. The record-breaking mRNA COVID-19 vaccine development was only possible through approximately 30 years of basic research investment across NIH to understand mRNA and how it could be applied in medicine, as well as many years of research on coronavirus biology and vaccine development. This effort, coupled with BARDA's prior investments in mRNA-based vaccine development and manufacturing for Zika, allowed for a rapid pivot of technology to address the COVID-19 outbreak. Accelerating development and commercialization was further made possible by BARDA's extensive investment in advanced development, utilization of longstanding NIH clinical trials networks, and the prioritization of FDA regulatory resources towards COVID-related tools.

To help replicate this success for any future pandemic, NIH will make significant investments to accelerate early-stage discovery, design, and development of vaccines and vaccine platforms, therapeutics, and adjuvants. ASPR will further support late-stage development and manufacturing of vaccines against high-consequence threats—including investments for pandemic influenza and other Emerging Infectious Diseases (EID), Sudan Virus (SUDV) and Marburg Virus (MARV), and other viruses with pandemic potential. ASPR will also invest in late-stage development and manufacturing of therapeutics – including those that that target SUDV and MARV, broad-spectrum antivirals and host-directed therapeutics, and new rapid response therapeutic platform technologies. Additionally, to ensure these innovations can be fully leveraged by the public, ASPR will also invest in advancing manufacturing capacity and securing needed supplies. These investments will secure additional mRNA manufacturing capacity, develop and advance new technologies in manufacturing, enhance bulk and fill/finish manufacturing for viral vectors, and help build a resilient supply chain and maintain key products within

the Strategic National Stockpile. Finally, to track effectiveness, safety, and utilization of such medical defenses, this funding will allow CDC to invest in its Medical Countermeasures Effectiveness Network.

And, to build core capabilities cutting across all pandemic preparedness work, ASPR will additionally support program management and mission execution, including by obtaining the required response personnel and information technology products and services. FDA will additionally invest $670 million to help build the regulatory capacity needed to support the activities above.

Administration for Strategic Preparedness and Response

Advanced development and licensure of vaccines, therapeutics and diagnostics against viral families with the highest pandemic potential

Vaccines: Development of faster pandemic influenza and other Emerging Infectious Disease (EID) vaccine response capability and enhanced manufacturing capacity. This funding will enable BARDA to rapidly address the need for a faster vaccine platform to respond to pandemic influenza which currently relies on recombinant, cell- and egg-based manufacturing, none of which allow for the required rapid manufacturing of strain-matched vaccines to meet the challenges of evolving influenza viruses, including the H5N1 clades that are currently circulating in birds and mammals. BARDA will invest in domestic mRNA vaccine manufacturing capacity and advancement of an mRNA-based pre-pandemic influenza vaccine to licensure. To exercise this manufacturing and development capacity, the agreement will include advanced development of at least three additional vaccines against viral families with pandemic potential for which licensed vaccines do not currently exist, such as Lassa, Nipah, Rift Valley Fever and others.

Vaccines: Advanced development of Sudan Virus (SUDV) and Marburg Virus (MARV) vaccines. The frequency of filovirus (Ebola, Sudan, Marburg and other viruses) outbreaks has increased in recent years with four outbreaks in 2022 and another already in 2023. In addition to the outbreak potential inherent in the increased frequency of emergence via spillover from natural reservoirs and re-emergence of human-to-human transmission in regions that have recovered from recent outbreaks, the filoviruses also have been determined to be a material threat to national security by the Department of Homeland Security. Due in part to supplemental funding that was provided to accelerate the development of p medical countermeasures against Ebola Zaire, the species that caused the 2014 West African outbreak, BARDA successfully advanced several MCMs to FDA licensure (e.g., ERVEBO, INMAZEB and EBANGA). Funding will leverage lessons learned from the development of these countermeasures to rapidly advance SUDV and MARV vaccines to FDA licensure and build stockpiles of each that will be sufficient to respond to domestic and international outbreaks.

Vaccines: Advanced development of additional vaccines that protect against viruses with pandemic potential. Recognizing that the mRNA vaccine platform may not be the best approach for all viruses with pandemic potential, BARDA will also support advanced development of 4-6 vaccine candidates produced using non-mRNA platforms (e.g., VSV, ChAd3, protein antigen, and others). The vaccine candidates will be selected from both existing candidates for which advanced development funding is not available and for novel vaccine candidates developed by NIH/NIAID as part of its work to support pandemic preparedness, further discussed below. As part of this effort, this funding will also support the advancement of 1-2 vaccines to FDA approval.

Therapeutics: Advanced development of Sudan Virus (SUDV) and Marburg Virus (MARV) therapeutics . As stated above, the filovirus family continues to be one of the largest pandemic threats the world faces. This funding will support advanced development and FDA approval of therapeutics against SUDV and

MARV and also support manufacturing of a stockpile of treatment courses for disease caused by both viruses that, based on recent history, will be sufficient to address naturally occurring outbreaks.

Therapeutics: Advanced development of broad-spectrum antivirals and host-directed therapeutics . ASPR will implement robust antiviral and threat-agnostic therapeutic programs by developing both pathogen-directed antivirals that inhibit key viral functions as well as host-directed therapies capable of mitigating the outcomes of severe disease. Preferred antivirals will target entire virus families, thus allowing development of products that can protect against known and unknown threats. Proposed viral targets include antivirals that could be efficacious in the treatment of disease caused by *Arenaviridae* viruses. Threat-agnostic approaches will target acute respiratory distress syndrome or other severe outcomes of infectious disease and candidates can be placed into a phase 2 platform trial within 12 months of funding being made available. Candidate drugs will have the ability to alleviate symptoms of disease, prevent severe disease and hospitalizations, and/or lower mortality.

Therapeutics: Advancement of new rapid response therapeutic platform technologies. New technologies and approaches are needed to accelerate therapeutic development and decrease costs. These include accelerating development of small molecule antiviral candidates to shorten the two years it took for COVID-19 oral antivirals to become widely available. Similarly, monoclonal antibodies, while currently our best option for several viral families, have cost and technology barriers that prevent them from reaching their full potential. An array of new technologies has been developed that could overcome these challenges, such as utilizing mRNA to express monoclonal antibodies and leveraging CRISPR and siRNA technologies to eliminate viral infection. Utilizing pathogens, including filoviruses and other pathogens of high pandemic potential, as targets, BARDA will incorporate these new platform approaches into the advanced development portfolio of therapeutics. This will not only provide MCMs against these known threats, but it will also support broader US innovation in the manufacturing and product development sector, much as was done with mRNA in the vaccine sector.

Diagnostics: Advanced development of diagnostics. ASPR will develop threat agnostic pathogen Next Generation Sequencing (NGS)-based diagnostics for use in laboratory and remote settings, which is a cornerstone technology for rapid response in the National Biodefense Strategy. The envisioned clearance would include a pre-approved change protocol to allow rapid addition of a novel emerging pathogen to the reference database, thus enabling use of the technology in an emerging pathogen response. ASPR will also invest in development and clearance of high testing performance platforms for use in remote and access constrained environments, increasing access to testing and improving the quality of healthcare in these settings. Lastly, investments will be made to develop specific diagnostics to complement vaccine and therapeutic efforts discussed in this request, thus creating a full MCM toolbox that spans identification of cases, treatment of patients, and pre-exposure protection from infection for contacts and others at risk of infection.

Biologics Manufacturing and Supply Chain

Manufacturing of vaccines and other biological products in response to a public health emergency is critical. In an outbreak response, supply chains and manufacturing capacity often become rate limiting. To address this gap, BARDA has developed plans for a Biopharmaceutical Manufacturing Partnership (BioMaP). This partnership seeks to strengthen the U.S. government and industry's response to current and future public health emergencies by strengthening and expanding the critical enabling capabilities and infrastructure–physical facilities, workforce training, supply chain, and manufacturing platforms–required for a robust and nimble vaccine-based response. Funding will be critical for this effort to successfully launch as currently envisioned – to both address recommendations from the 2023 GAO report on planning for medical countermeasures (MCM) development and manufacturing risks, as well as fund the

required manufacturing capacity reservation. In short, this funding will allow the program to have a significant and immediate impact on the Nation's pandemic preparedness and response capabilities. The focus will include three efforts, each of which is specifically designed to complement the previously described vaccine development efforts:

Securing additional mRNA manufacturing capacity and maintaining capabilities developed during COVID-19 response . This action will secure additional manufacturing capacity for mRNA-based vaccines which will ensure that the Nation can avoid supply chain issues similar to the 2004-2005 influenza vaccine shortage, retain ability to meet surges in demand that would occur if a more virulent SARS-CoV-2 strain emerges and rely on domestic rather than international manufacturing during a period of crisis. This capacity/capability will be "exercised" twice annually to pressure test its ability to rapidly advance new vaccines on a compressed timeline in alignment with the National Biodefense Strategy and other US and Global objectives (e.g., American Pandemic Preparedness Plan, 100 Days Mission, etc.). These "exercises" will complement the product-specific development plans described earlier and be applied to candidate vaccines for pandemic influenza and other viruses with high pandemic potential and, in addition to confirming processes, staff and critical infrastructure are ready for rapid response when needed, this strategy will accelerate development of novel vaccines and produce limited stockpiles of doses that can be used for clinical trials and, as appropriate, outbreak response.

Innovation in manufacturing and other technologies. Develop and advance new technologies and approaches that will reduce the time to first dose, reduce costs, and shrink manufacturing footprint. In many instances, promising technologies have been discovered, but lack of funding has prevented rapid advancement and integration into cGMP manufacturing. Funding may also be used to develop new technologies to improve biosurveillance and early warning systems to enable rapid response to emerging threats.

Bulk and fill/finish manufacturing for viral vectors over a four-year period. Many companies are developing vaccines against viruses with pandemic potential based on different viral vector platforms. Advanced development of these platforms is slowed in part by lack of access to specialized manufacturing and fill/finish capability necessary to produce these products. Further, these efforts, when they do occur, are spread amongst multiple manufacturers, preventing both economies of scale, as well as 'lessons learned' from being broadly applied. Addressing this gap via partnership with contract manufacturing organizations, pharmaceutical companies and other industry partners will have an out-sized impact on vaccine advanced development.

Industrial Base Management and Supply Chain and Strategic National Stockpile. Funding will advance pandemic preparedness as it relates to personal protective equipment and critical medicines supply chain resiliency, maintenance of key holdings within the Strategic National Stockpile, expanded distribution capacity, and efforts designed to alleviate stresses to national supply chains for critical products (e.g., syringes, needles, vials, stoppers, etc.) during outbreak/pandemic response.

Managing the mission

Program Management. Funding will support personnel and information technology products and services required for the execution of the scope described here, coordination across HHS and reporting to the Office of the Secretary of HHS and other US Government stakeholders.

Centers for Disease Control and Prevention

To create the conditions for speed, effective and scalable preparedness and response systems must be put in place long before emergencies strike. However, these systems are beyond the scope of current agency base budgets. Making strategic investments based on these lessons during the pandemic would set

America's public health system on a path to save countless lives and livelihoods in the future. Starting in FY 2024, CDC proposes a **$6.1 billion investment in preparedness.** With these resources, CDC will modernize and build laboratory capacity and strengthen public health data systems; enhance domestic and global disease surveillance, biosafety, and biosecurity efforts; and support capabilities for monitoring and evaluating vaccine and medical countermeasure safety, effectiveness, and utilization.

Early detection of emerging pandemic threats is the foundation for rapid response and countermeasure development activities. Public health surveillance provides an ongoing picture of the patterns of disease, which is critical to implementation and evaluation of control measures and detection of new and emerging threats. Since pathogens do not recognize international borders, public health surveillance cannot stop at the border either. For the United States to be prepared for a pandemic, we must support and contribute to a globally connected network of public health surveillance systems. This proposal would make investments across CDC to help detect new pathogens or variants weeks or months earlier. This investment would strengthen existing surveillance programs as well as build novel, pathogen-agnostic approaches like rapid genomic sequencing directly from clinical samples, so that we can get more and faster information from a sample. Investments would expand support for sentinel surveillance systems, novel pathogen-agnostic approaches, and influenza-like illness and other respiratory disease surveillance. With this funding, the United States could also **significantly increase** our investments in early warning including by the addition of **thousands** more wastewater testing sites across the country to increase geographic representation and breadth/depth of sampling and allow for the addition of facility-based testing sites (e.g., in nursing homes, other congregate settings, and more). Techniques and infrastructure involving metagenomics, for example, that sequence a collection of genes in a single sample without the need for isolation or lab cultivation of a specific species, could greatly improve the speed and quality of clinical and public health decision making.

Modernizing the public health data system is critical to pandemic preparedness as it supports the sharing of complete, accurate, and timely information essential for detecting and controlling emerging threats. To address long-standing deficits, CDC will invest in improving bidirectional data flow to bring more timely and complete information through these data systems, reducing the burden on data providers, and enhancing access by STLT users as well as CDC and our federal partners. This will provide high-quality information that will support decision makers with early warnings and insights into outbreaks.

This funding will also invest in integrating and improving the nation's public health laboratory system. It will improve the physical infrastructure and technologic capacity to enable large-scale response without compromising other ongoing critical activities. It will also allow public health laboratories around the nation to operationalize surge testing when needed, and support partnership between clinical and public health laboratories to improve speed and depth of pathogen detection.

To mitigate the risks associated with advanced international laboratory capacity, CDC will work with its partners to accelerate the adoption of biosafety and biosecurity practices at the regional, national, and subnational levels, such as improving the safe and appropriate handling, testing, storage, and transportation of unknown pathogens.

Finally, after products are authorized, we must have real-world data on safety, effectiveness, and utilization of MCMs to inform usage, and guide rapid, equitable prioritization and distribution of these tools. Funding will also be used to invest in CDC's Medical Countermeasures Effectiveness Network for monitoring of vaccines and therapeutics, Vaccine Safety Network monitoring of post-illness conditions and modernization, and MCM distribution network improvements. As just one example, investments will help expand and automate vaccine safety monitoring systems by utilizing electronic health records to increase the volume of data going into the system, while decreasing the burden on healthcare providers.

National Institutes of Health

Early detection and response

Recent responses have highlighted the importance of having wide availability of diagnostics early in a response. This proposal includes funding to support the Rapid Acceleration of Diagnostics (RADx) initiative's highly effective Innovation Funnel and Independent Test Assessment Program (ITAP). Between 2020 and 2022, RADx accelerated design, validation, regulatory authorization, and manufacturing of point of care (POC), over the counter (OTC), and laboratory COVID-19 tests, leading to 50 emergency use authorizations (EUAs) and increasing national capacity by >5 billion tests. These technology advances would be leveraged in order to develop next-generation POC and OTC home diagnostics that target high-priority pathogens and diseases, with a focus on improving rapid home test performance to match laboratory-level accuracy, reducing test cost and accessibility barriers, detecting multiple pathogens at once, and advancing digital health platforms for at home "Test to Treat" and test reporting programs.

Funding also supports RADx's ITAP collaboration with the FDA to accelerate authorization and clearance of new tests, using standardized methods and protocols to reduce time to authorization to as little as two months. ITAP would also continue to gather data needed by FDA to support decision-making, including assessing authorized platforms for performance with new variants and pathogens, and getting real world evidence to inform use guidance and next-generation design.

and pathogens, and getting real world evidence to inform use guidance and next-generation design.

Protective countermeasures

Building on the vaccine development successes of the COVID-19 pandemic, funding will support efforts directed at several pathogens of concern along the full R&D continuum. This investment will accelerate early-stage discovery, design, and development of vaccines and vaccine platforms, therapeutics, and adjuvants.

Though the precise nature of the next threat is unknown, we know that climate change and habitat disruption are increasing contact between humans and animal reservoirs of diverse pathogens, enhancing the likelihood of spillover events leading to epidemics and pandemics. We also know which viral families pose the greatest risk of sparking a pandemic and must advance our foundational understanding of representative pathogens from each of these families simultaneously.

The request will support NIH's preclinical R&D, similar to the foundational work completed in the decades leading up to the COVID-19 vaccine development; expand laboratory capacity and pilot cGMP manufacturing infrastructure for phase 1/2 clinical studies of candidates discovered through preclinical initiatives; and fund Phase 1 and 2 clinical trials to evaluate safety and immunogenicity of the most promising vaccines and therapeutics (including host-tissue-directed therapeutics), which can be transitioned to ASPR/BARDA or other advanced development partners for late stage development. Funding will establish, expand, and/or improve large and rapidly scalable clinical trials networks and infrastructure to generate real-world evidence on the performance of vaccines, therapeutics, and diagnostics. And, to support the safe and secure conduct of all early-stage activities, we propose biosafety and biosecurity investments that will sustain the capabilities and increase the availability of BSL-3/-4 laboratories.

Food and Drug Administration

The COVID-19 pandemic has reiterated FDA's unique and cross-cutting role, which is central to the whole-of-government response to protect and promote public health. The Budget provides $670 million

to improve FDA's core capabilities and regulatory capacity to respond rapidly and effectively to any future pandemic or internationally significant biological incident. To maintain FDA's gold standard for science-based product review and regulatory decision-making, the Budget will help modernize FDA's regulatory capacity, information technology, and laboratory infrastructure.

These funds would support the Agency's biodefense efforts, domestic and globally, by bolstering FDA's cadre of medical product reviewers and strengthening foundational processes. It would also increase FDA's capacity to leverage a One Health approach to respond to emerging threats in recognition of the inter-connectedness of human, animal, and environmental health. The Budget also will improve FDA's laboratory facilities so that FDA has modern and safe physical spaces necessary to conduct our regulatory pandemic preparedness and response work.

And lastly, these resources would help strengthen underlying technology platforms to improve electronic information exchange among stakeholders. The funding will further build FDA's data infrastructure capabilities such as advanced predictive modeling data analytics capacity, real-world data analysis tools, and business continuity systems. With these resources, FDA will have the opportunity now to build on lessons learned and provide transformational investments to help ensure that FDA can respond quickly and effectively in times of a public health crisis.

OVERVIEW OF PREPAREDNESS LEGISLATIVE PROPOSALS

HHS had to overcome real administrative challenges and a patchwork of authorities and flexibilities while responding to the once-in-a-century COVID-19 pandemic and other recent emergencies, including the infant formula shortage and Hurricanes Ian and Fiona. The 2024 Budget includes legislative proposals to improve preparedness and response, incorporating lessons learned from these recent public health emergencies. Together, the proposals discussed below will help bridge key gaps and barriers to enable a robust and timely response to future emergencies. These proposals complement discretionary investments and the $20 billion in mandatory funding requested across HHS public health agencies to prepare for pandemics and other biological threats. Additional information about these proposals may be found in the respective Operating Division's Congressional Justification.

1. Early detection and response

Data and laboratory capacity

New authorities are needed to address challenges HHS faces in getting high-quality data needed to quickly identify and respond to new public health threats. For example, during COVID-19, it took six months for CDC to get jurisdictions to agree to sign 61 Data Use Agreements before the federal government could get critical data from jurisdictions—and in some cases it took 18 months to two years to negotiate with a state or local immunization information system. Notwithstanding any other provision of law, the Secretary will have the new authority to require data from health care providers, facilities, suppliers, pharmacies, laboratories, service organizations, and state, local, Tribal, and territorial agencies, for the purposes of public health threat detection and monitoring; evaluation and distribution of medical countermeasures and critical supplies; and connection of communities with resources and services. This authority will allow for more complete and timely data sharing to support decisions at the federal, state, and local levels. Data collection will be coordinated across HHS agencies to minimize reporting burden and be subject to federal privacy and security protections to protect confidentiality.

To support scaling of laboratory capacity itself, we also propose a **domestic construction authority for ASPR and CDC**, allowing the construction and alteration of non-federally owned facilities to support public health requirements. This authority could provide grants for construction and major renovation of public health labs to support early detection, as included in the CARES Act (this is coupled with construction authorities supporting medical countermeasures [MCMs] and supplies, discussed later).

Supply risks and accountability

To support identification and monitoring of potential and existing drug shortages, we propose expanding authorities to require drug manufacturers to **notify FDA of drug demand increases** that manufacturers are unlikely to meet. This would supplement existing data on supply-side

disruptions that may result in shortages. Allowing FDA to require **enhanced drug manufacturing amount information**—namely, identification of suppliers relied on to manufacture drugs and the extent of such reliance, would further allow FDA to better work with manufacturers proactively to diversify their supply chain. Additionally, we seek authority for FDA to require **Site Master Files (SMFs) for Drug Manufacturing Facilities,** which will assist FDA when conducting risk identification for sites for surveillance and for-cause inspections. Requiring the SMFs for facilities manufacturing also has the potential to make inspections more efficient.

To help address identified drug shortages, we also propose **providing FDA the authority to require expiration dates to be lengthened to mitigate critical drug shortages**. This authority would allow FDA to require, when likely to help prevent or mitigate a shortage, that an applicant evaluate, submit data to FDA, and label a product with the longest expiration date (shelf-life) that is scientifically justified and include that failure to comply is a prohibited act and authority for FDA to levy civil money penalties.

A recent focus on firms manufacturing non-application drugs has identified a high rate of non-compliance with current good manufacturing practice (CGMP) requirements, especially when a facility is first inspected. To address this**, FDA is seeking authorities with respect to non-application drugs** (finished dosage forms and active pharmaceutical ingredients) to provide the agency time to determine if an inspection of the manufacturing facility is necessary before the drug can be distributed, and to conduct the inspection.

Beyond drugs, we also propose amending the Federal Food, Drug, and Cosmetic Act **authorities to help identify and address critical device shortages,** which proved deadly early in the COVID-19 pandemic. This includes requiring firms to both notify FDA as soon as possible after an interruption in the manufacturing of a critical device—not just during or in advance of a declared public health emergency—and to implement other mitigation steps. Without this amendment, FDA's ability to proactively respond to early signs of supply constraints or a potential shortage situation will be limited in situations like recalls, cyberattacks, and natural disasters that may not lead to the declaration of a public health emergency but which can result in significant device shortages and impact patient care. This proposal would also provide FDA the clear authority to review risk management plans (RMPs) for critical devices to help ensure manufacturers have plans in place to enhance resiliency and mitigate future supply chain disruptions. .

We also propose similar authorities for FDA to require firms to **notify FDA of food shortages.** FDA is seeking authority to require firms to provide shortage notification for FDA-designated categories of food during a declared public health emergency. The recent COVID-19 pandemic has demonstrated the need for timely and accurate information about confirmed or likely supply chain challenges to help ensure the continuity of the food supply so that consumers have access to a safe and adequate food supply during public health crises. .

2. **Safe, effective medical countermeasures (MCMs) and supplies**

Before the development of the first COVID-19 mRNA vaccine in less than a year, the fastest vaccine to go from development to deployment was for mumps, taking four years. Much of this

success is due to unprecedented financial investments, interagency collaboration, and years of foundational vaccine research and development. However, several authorities made available to HHS uniquely during the COVID-19 public health emergency helped make these accomplishments possible. At present, many of these authorities are not available for the next public health emergency, and additional authorities would further strengthen our ability to bridge gaps in ensuring availability and access to MCMs and other critical supplies.

Innovative research and development

To build on our R&D successes and best leverage our investments in medical countermeasures, we propose expanded authorities to foster public-private innovation. This includes **permanently extending BARDA's Medical Countermeasures Innovation Partner (MCIP) Authority**. This authority allows the USG to partner with nonprofit entities to use venture capital practices to address health security needs.

To help bring these promising products through authorization and/or approval, we propose **providing FDA the explicit authority to establish a Pandemic Preparedness Program** to enhance regulatory capabilities and readiness to rapidly review new vaccines and other medical products in response to emerging pathogens. In consultation with Health and Human Services partners, the program would: provide recommendations and guidance to developers of vaccines and other medical products and relevant federal partners; use real-world data or real-world evidence to study the safety and effectiveness of products for addressing biological incidents and identify which products may be best suited for specific pathogens or for use in different populations; and facilitate product development including advances in manufacturing.

Manufacturing and availability

Readily available, large-scale, domestic manufacturing capability accelerates response. To ensure adequate domestic manufacturing capacity of MCMs and supplies, we propose authorities for HHS to use funding in ways that effectively support sustainment of existing manufacturing capacity and expansion of new domestic capacity. **Authority for acquisition, construction, or alteration of non-federally owned facilities** would allow ASPR to support efforts to develop net new domestic manufacturing capacity for MCMs and related products, in addition to allowing CDC to support public health laboratory improvements discussed above to support early detection and response. Currently, this authority is often granted in emergency supplemental appropriations acts, which means constructed/altered facilities can only support a specific product—this is inefficient as manufacturing lines can often be flexed for different products. This authority would both ensure HHS's ability to support cross-cutting manufacturing investments, and to make these investments when they're needed.

Procurement and acquisition

At the outset of the pandemic, HHS did not have the authority to execute acquisitions and contracting actions as quickly or efficiently as needed to ensure widespread access to needed supplies. For example, HHS does not have the authority to award follow-on production contracts from prototypes without recompeting the requirements; this authority was used by the

Department of Defense (DOD) to procure 5 of the 6 COVID-19 vaccines on behalf of HHS. HHS also does not have the authority to procure experimental supplies, including diagnostic reagents and ancillary supplies like needles and syringes to be used in the development of the best supplies, and lacks contracting mechanisms like the DOD's commercial solutions opening authority that can facilitate rapid and efficient acquisition of technology and services in a response. HHS had to form and rely on a partnership with the DOD to get the supplies and services it needed, at the speed required for response. This partnership was a critical asset during COVID-19 response, but DOD's surge support is ending and has been transitioned to the Administration for Strategic Preparedness and Response's (ASPR) HHS Coordination Operations and Response Element (H-CORE). HHS will no longer have access to these authorities without relying on DOD, including for the next public health emergency.

To support procurement of these products and critical supplies, as well as the tools and services to distribute them, we must codify the successes of HHS's partnership with the DOD over the course of the COVID-19 pandemic. We propose expanding ASPR's **Other Transaction Authority (OTA)** such that ASPR could fund development of a product—likely a vaccine, therapeutic, or diagnostic—and then move directly into large-scale manufacturing of the product, whether for a response or for stockpiling, reducing timelines to begin production by months.

To better position HHS to rapidly acquire the quantities of supplies needed for experimentation, technical evaluation, and strong operational capabilities in future emergencies, without relying on DOD or other Federal agencies, we also propose **providing ASPR the authority for procurement and acquisition of supplies for experimental or test purposes**, similar to that of DOD's. These materials and assets would include chemical materials and reagents, medical supplies, PPE, and ancillary supplies (e.g., needles and syringes) for the development of supplies needed for national public health and health security.

Further, **providing ASPR the authority to acquire innovative commercial products, services, processes, and/or methods**—like the DOD's Commercial Solutions Opening authority—would allow ASPR to acquire products or services such as technology investment agreements, research and development activities, and other capabilities needed to respond to an outbreak in the future without relying on other Federal agencies.

Access and adoption

Increasing availability of needed products and services alone is not sufficient for effective response; investing in the infrastructure that provides access and facilitates adoption is critical. As demonstrated in the pandemic response, no-cost products and services drives equity in adoption and ultimately outbreak control of vaccine-preventable diseases. To learn from the successful focus on equity during recent responses, we propose **providing CDC with the legislative authority and funding to establish the Vaccines for Adults program** to begin expanding access to Advisory Committee on Immunization Practices (ACIP)-recommended routine and outbreak vaccines for uninsured adults at no cost. This capped mandatory program would be modeled on the successful Vaccines for Children (VFC) program and tailored to meet the unique needs of adults, and would fund the purchase of ACIP-recommended vaccines for eligible adults, provider fees, and program operations.

To further support broader access to medical products and services directly related to diagnosis, treatment, and/or prevention (such as immunization) of specific disease or conditions that are pandemic-related as determined by the World Health Organization, we also propose **modifying Section 1135 emergency waiver authorities to ensure Medicare, Medicaid, and CHIP beneficiaries and the uninsured have access to critical products and services, including unapproved drugs, vaccines, and devices in a pandemic.** Under this proposal, the Secretary could authorize or require coverage of unapproved drugs, vaccines, or devices, that are authorized by FDA for emergency use, or other items and services used treat a pandemic disease during a public health emergency (PHE). Patient cost-sharing would be waived for vaccines authorized under an EUA, and the administration of such vaccines. Reconciliation may be used to make Part D and Part C plan sponsors whole for drug, vaccine, device, and administration costs –including costs associated with vaccine counseling— that were not incorporated in their bids, if the cost is estimated to exceed 0.1 percent of the national average per capita costs. The Secretary will provide Congress certification and advance written notice before exercising this authority.

Safety and accountability

Lack of transparency has constrained accountability for safety and efficacy of critical supplies—for example, FDA often cannot always trace manufacturers along the supply chain to hold them accountable. FDA also cannot require advance records or remote inspections or share critical data with states without manufacturer consent, limiting inspection efficiency and the ability for states to support investigations.

We propose allowing FDA to **require labeling to include the original manufacturer and supply chain information**. This authority could support investigations in events such as during the COVID-19 pandemic, when methanol contamination in active pharmaceutical ingredients (API) for hand sanitizer led to more than 20 deaths—in that event, were not able to identify original API manufacturers and hold them accountable.

We also propose **expanding FDA's existing oversight authorities** vis-à-vis drug manufacturers to all FDA-regulated product manufacturers. This proposal would allow FDA to request records or other information in advance of or in lieu of inspections from manufacturers of any FDA-regulated products, improving efficiency of any subsequent inspections by helping to identify specific risks on which to focus inspectional time. This proposal would also allow FDA to require—not just request—remote evaluations, which have helped FDA verify post-inspection corrective actions have been taken and otherwise gain compliance insight.

To support safety of other medical products, we propose an authority to **expand FDA information disclosures with states**. This proposal would facilitate FDA sharing non-public information with states, territories, or localities, without manufacturers' express consent, to support joint inspections of firms, inventory, and distribution records. The ability to collaborate with state partners would allow FDA to focus on enforcement where it is needed most, such as investigations of fraudulent medical products. This proposal would also advance an integrated food safety system and more effective use of federal and state oversight tools.

3. Resilient public health and health care systems

Attracting, hiring, and retaining workforce

Traditional mechanisms are not sufficient to fill positions rapidly and maintain them during public health emergencies. The COVID-19 pandemic has also exacerbated the estimated global shortage of 18 million health workers by 2030. To provide HHS with the ability to quickly fill relevant positions in the event of future public health emergencies—including to detect threats and support development and procurement of the tools needed to respond—we propose a **Direct Hire Authority for ASPR and CDC during Public Health Emergencies** for mission critical professionals. This would include for skills in specialized biological sciences, emergency management, and acquisitions – allowing HHS to reduce time to hire when it matters most. We similarly propose **extending the National Disaster Medical System Direct (NDMS) Hire Authority**, which will expire in September 2023—this authority has successfully expanded the NDMS intermittent workforce by approximately 25% and cut hiring time in half (from an average of one year to six months).

Ability to hire is insufficient without the ability to attract workforce with competitive offers. We propose authorizing appropriate and flexible pay authorities to allow HHS and its agencies (CDC and ASPR in particular) to provide compensation that is more competitive with market salaries and improve recruitment and retention of individuals with mission critical positions. This would include authority for HHS to provide **overtime and danger pay** to any employee serving with threat to well-being and to **waive the statutory pay cap on aggregate basic and premium pay during a public health emergency** (as reflected in HHS's General Provisions). And, to better attract clinicians and other highly sought-after technical experts, we propose a **student loan repayment tax code exclusion for CDC's Education Loan Repayment Program for Health Professionals**, like HRSA's National Health Service Corps (NHSC) authority. This would relieve CDC of a high tax burden on a key talent recruitment mechanism— the true cost to CDC for $100,000 in loan repayment is nearly $150,000 due to the fact CDC has to pay taxes on behalf of the individual and the employer portion of Social Security and Medicare in addition to the loan repayment. Savings could be used to recruit more public health workers.

We also propose allowing CDC to **waive maximum hour/dual compensation restrictions for reemployed annuitants (REA)** for up to one year: This would allow CDC to fully use the skills and expertise of reemployed annuitants to fill full-time roles in emergency responses and work the hours needed to meet emergency response needs during a declared PHE response.

Finally, to allow us to further supplement our workforce with volunteers, we propose **amending the authority for the Medical Reserve Corps (MRC) Program.** Notably, the authority to deem MRC volunteers as time-limited Federal employees for purposes of liability coverage and medical license credentials would support greater staffing pools for CDC, ASPR, and others broadly. This would allow us to better tap into over 300,000 MRC volunteers nationwide for federal responses such as hurricanes.

Optimizing existing capacity

In addition to attracting and retaining workforce, optimizing existing capacity is a critical lever for building adaptive public health systems. For this, we propose allowing CDC to dedicate a small percentage of funding across CDC's appropriations for the purpose of funding **a response-ready cadre of staff** who can quickly deploy for any Public Health Emergency or other emerging threats, and then return to their regular duties when the event is resolved. Without this authority, CDC is limited in its ability to rapidly engage its full workforce to support an emergency response because only staff whose regular positions are funded by appropriations consistent with prospective response duties can undertake those activities without formal personnel processing. In addition, even when CDC's Emergency Operations Center (EOC) is formally activated, which allows all CDC staff to support the EOC without reimbursement, there are still current limitations such as a limit on the length of the detail assignments and required Congressional tracking and reporting of all staff supporting the EOC.

4. Enhancing recovery

Capacity building and response authorities

Programs need but often do not have the funding authorities and flexibilities to support coordinated, targeted human services delivery following a disaster. We propose to **establish a disaster human services emergency fund** to strategically respond to disasters by promptly directing funds to support disaster-caused human service needs. This fund would also address issues related to fiscal year limitations by allowing for funding for disasters occurring near the end of the fiscal year—which overlaps with Atlantic hurricane and Western wildfire seasons. Using this fund to help meet surges in service demands, recover from losses, and address immediate needs would significantly improve disaster response for some of the most vulnerable populations, including people with disabilities, older adults, children and families.

We also propose authorities to **provide comprehensive case management services,** to address survivors' additional human services needs arising during crisis response to achieve stability. Currently, HHS (via ACF) is constrained in the scope, scale, and frequency of case management services it can provide to disaster survivors. This mechanism would complement the disaster human services emergency fund and reduce further harm to disaster survivors by ensuring resources and services are linked through a robust, coordinated continuum of care.

5. Cross-cutting priorities

Flexibility to manage funds and waive certain statutory requirements are cross-cutting needs for effective operations. We propose providing ASPR the authority to **establish a working capital fund**, to ensure resources are available to fully support administrative requirements, even through periods of funding uncertainty and surge operations. The working capital fund will help cover ASPR's requirements across information technology, human resources, and financial management including acquisition policy and oversight.

NONRECURRING EXPENSES FUND

Office of National Security

Budget Summary

(Dollars in Thousands)

	FY 2022	FY 2023[3]	FY 2024[3]
Notification[4]	--	$1,900	$7,200

Authorizing Legislation:

Authorization .... Section 223 of Division G of the Consolidated Appropriations Act, 2008

Allocation Method ....Direct Federal, Competitive Contract

Program Description and Accomplishment

The Nonrecurring Expenses Fund (NEF) permits HHS to transfer unobligated balances of expired discretionary funds from FY 2008 and subsequent years into the NEF account. Congress authorized use of the funds for capital acquisitions necessary for the operation of the Department, specifically information technology (IT) and facilities infrastructure acquisitions. The Office of National Security (ONS) will enhance established programs to take a more proactive role toward our national security mission and protecting the Department.

Budget Allocation FY 2024

The following projects are planned uses of the NEF for ONS in FY 2024, totaling $7,200,000:

Sensitive Compartmented Information Facility (SCIF) Expansion

ONS plans to expand the SCIF in the Humphrey Building due to increased workload and staff levels. The expanded space will add areas to currently existing space and will support the current and new programs and staff as well as provide enough room for interdepartmental partners to work collaboratively.

ONS Case Management System

ONS NEF funds will be used to add a case management system within its secured network to ensure Insider Threat, Counterintelligence, and Intelligence & Analysis teams are able to secure their information on one platform. This update will allow users to conduct internal research and analysis (with query capability), secure information access to need-to-know, and house a record of cases.

Technical Surveillance Countermeasures (TSCM) Program Equipment Refresh

The ONS TSCM Program is required to ensure equipment is updated every three years. Currently, much of the equipment is beyond five years old and considered out-of-date. To meet the current TSCM standards updated equipment is needed.

Budget Allocation FY 2023

Enterprise Supply Chain Risk Management System - $1,900,000

NEF funds are used to purchase an Enterprise Supply Chain Risk Management system/platform licenses for research, analysis and assessment development for vulnerable HHS acquisitions.

---

[3] Notification submitted to the Committees on Appropriations in the House of Representatives and the Senate on September 23, 2022. [3] This represents the total amount to be notified as a planned use of funds in a FY 2024 notification letter.

[4] Pursuant to Section 223 of Division G of the Consolidated Appropriation Act, 2008, notification is required of planned use.

IDEA DIGITAL MODERNIZATION ACT

Modernization of the Public-Facing Digital Services – 21st Century Integrated Digital Experience Act

The 21st Century Integrated Digital Experience Act (IDEA) was signed into law on Dec. 20, 2018. It requires data-driven, user-centric website and digital services modernization, website consolidation, and website design consistency in all Executive Agencies. Departments across the federal landscape are working to implement innovative digital communications approaches to increase efficiency and create more effective relationships with their intended audiences. The American public expects instant and impactful communications – desired, trusted content available when they want it, where they want it, and in the format they want it. If the consumer is not satisfied, they move on and our opportunity for impact is lost.

Modernization Efforts

In FY 2019 HHS engaged Department leadership and developed a Digital Communications Strategy that aligns with the requirements of IDEA. In FY 2020, HHS Digital Communications Leaders began implementation of the Strategy in alignment with IDEA, beginning to align budgets to modernization requirements.

As the result of a comprehensive review of costs associated with website development, maintenance, and their measures of effectiveness, HHS will prioritize:

- modernization needs of websites, including providing unique digital communications services, and
- continue developing estimated costs and impact measures for achieving IDEA.

Over the next four years HHS will continue to implement IDEA by focusing extensively on a user-centric, digital first approach to both external and internal communications and developing performance standards. HHS will focus on training, hiring, and tools that drive the communication culture change necessary to successfully implement IDEA.

Over the next year, HHS Agencies and Offices will work together to continue to implement IDEA and the HHS Digital Communications Strategy across all communications products and platforms.

SUPPLEMENTAL MATERIAL

Budget Authority by Object Class

Description	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2023 +/- FY 2022
Personnel compensation:				
Full-time permanent (11.1)	20.428	22.407	30.312	+7.905
Other than full-time permanent (11.3)	0.170	0.185	0.578	+0.393
Other personnel compensation (11.5)	0.106	0.127	0.077	-0.050
Military personnel (11.7)	--	--	3.901	+3.901
Special personnel services payments (11.8)	--	--	0.000	+0.000
Subtotal, Personnel Compensation	**+20.704**	**+22.719**	**+34.869**	**+12.150**
Civilian benefits (12.1)	6.912	7.634	9.573	+1.939
Military benefits (12.2)	--	--	0.492	+0.492
Benefits to former personnel (13.0)	--	--	--	--
Total Pay Costs	**+27.615**	**+30.353**	**+44.933**	**+14.580**
Travel and transportation of persons (21.0)	0.164	0.320	0.941	+0.621
Transportation of things (22.0)	0.450	0.450	0.082	-0.368
Rental payments to GSA (23.1)	1.607	1.360	2.565	+1.205
Rental payments to Others (23.2)	--	--	0.029	+0.029
Communication, utilities, and misc. charges (23.3)	0.063	0.063	0.142	+0.079
Printing and reproduction (24.0)	0.001	0.001	0.000	-0.001
Other Contractual Services:				
Advisory and assistance services (25.1)	32.398	42.887	46.858	+3.971
Other services (25.2)	9.356	11.857	61.606	+49.749
Purchase of goods and services from government accounts (25.3)	7.293	9.452	19.086	+9.634
Operation and maintenance of facilities (25.4)	0.055	0.075	0.100	+0.025
Research and Development Contracts (25.5)	--	--	--	--
Medical care (25.6)	0.043	0.043	--	-0.043
Operation and maintenance of equipment (25.7)	7.656	18.155	101.005	+82.850
Subsistence and support of persons (25.8)	--	--	--	--
Subtotal, Other Contractual Services	**+56.801**	**+82.469**	**+228.65**	**+146.185**
Supplies and materials (26.0)	0.199	0.225	0.172	-0.053
Equipment (31.0)	0.506	0.750	0.800	+0.050
Land and Structures (32.0)	--	--	--	--
Investments and Loans (33.0)	--	--	--	--
Grants, subsidies, and contributions (41.0)	--	--	--	--
Insurance claims and indemnities (42.0)	--	--	--	--
Interest and dividends (43.0)	--	--	--	--
Refunds (44.0)	--	--	0.002	+0.002
Total Non-Pay Costs	**+59.791**	**+85.638**	**+233.387**	**+147.749**
Total, Budget Authority by Object Class	**+87.406**	**+115.992**	**+278.318**	**+162.328**

Note: The Public Health and Social Services Fund previously contained the annual appropriation for the Administration for Strategic Preparedness and Response (ASPR). The FY 2024 budget requests funding for ASPR in a separate, new appropriation account. This table is comparably adjusted to remove ASPR's programs from FY 2022 and FY 2023.

Salaries and Expenses

Description	FY 2022 Final	FY 2023 Enacted	FY 2024 President's Budget	FY 2023 +/- FY 2022
Personnel compensation:				
Full-time permanent (11.1)	20.428	22.407	30.312	+7.905
Other than full-time permanent (11.3)	0.170	0.185	0.578	+0.393
Other personnel compensation (11.5)	0.106	0.127	0.077	-0.050
Military personnel (11.7)	--	--	3.901	+3.901
Special personnel services payments (11.8)	--	--	0.000	+0.000
Subtotal, Personnel Compensation	**+20.704**	**+22.719**	**+34.869**	**+12.150**
Civilian benefits (12.1)	6.912	7.634	9.573	+1.939
Military benefits (12.2)	--	--	0.492	+0.492
Benefits to former personnel (13.0)	--	--	--	--
Total Pay Costs	**+27.615**	**+30.353**	**+44.933**	**+14.580**
Travel and transportation of persons (21.0)	0.164	0.320	0.941	+0.621
Transportation of things (22.0)	0.450	0.450	0.082	-0.368
Rental payments to GSA (23.1)	1.607	1.360	2.565	+1.205
Rental payments to Others (23.2)	--	--	0.029	+0.029
Communication, utilities, and misc. charges (23.3)	0.063	0.063	0.142	+0.079
Printing and reproduction (24.0)	0.001	0.001	0.000	-0.001
Other Contractual Services:				
Advisory and assistance services (25.1)	32.398	42.887	46.858	+3.971
Other services (25.2)	9.356	11.857	61.606	+49.749
Purchase of goods and services from government accounts (25.3)	7.293	9.452	19.086	+9.634
Operation and maintenance of facilities (25.4)	0.055	0.075	0.100	+0.025
Research and Development Contracts (25.5)	--	--	--	--
Medical care (25.6)	0.043	0.043	--	-0.043
Operation and maintenance of equipment (25.7)	7.656	18.155	101.005	+82.850
Subsistence and support of persons (25.8)	--	--	--	--
Subtotal, Other Contractual Services	**+56.801**	**+82.469**	**+228.65**	**+146.185**
Supplies and materials (26.0)	0.199	0.225	0.172	-0.053
Equipment (31.0)	0.506	0.750	0.800	+0.050
Land and Structures (32.0)	--	--	--	--
Investments and Loans (33.0)	--	--	--	--
Grants, subsidies, and contributions (41.0)	--	--	--	--
Insurance claims and indemnities (42.0)	--	--	--	--
Interest and dividends (43.0)	--	--	--	--
Refunds (44.0)	--	--	0.002	+0.002
Total Non-Pay Costs	**+59.791**	**+85.638**	**+233.387**	**+147.749**
Total, Salary & Expense	**+87.406**	**+115.992**	**+278.318**	**+162.328**
Direct FTE	**163**	**199**	**376**	**+177**

Note: The Public Health and Social Services Fund previously contained the annual appropriation for the Administration for Strategic Preparedness and Response (ASPR). The FY 2024 budget requests funding for ASPR in a separate, new appropriation account. This table is comparably adjusted to remove ASPR's programs from FY 2022 and FY 2023.

Detail of Full-Time Equivalent Employment

	2022 Actual Civilian	2022 Actual Military	2022 Actual Total	2023 Est. Civilian	2023 Est. Military	2023 Est. Total	2024 Est. Civilian	2024 Est. Military	2024 Est. Total
Cybersecurity	109	--	109	143	--	143	143	--	**143**
Office of National Security	36	2	38	36	2	38	54	2	**56**
Office of Global Affairs	16	--	16	18	--	18	20	--	**20**
Office of the Assistant Secretary for Health	--	--	--	--	--	--	16	131	**157**
Readiness Training	--	--	--	--	--	--	*2*	--	***2***
Ready Reserve	--	--	--	--	--	--	*14*	*117*	***131***
Public Health Emergency Response Strike Team	--	--	--	--	--	--	--	*24*	***24***
PHSSEF FTE Total	**161**	**2**	**163**	**197**	**2**	**199**	**233**	**143**	**376**

Note: The Public Health and Social Services Fund previously contained the annual appropriation for the Administration for Strategic Preparedness and Response (ASPR). The FY 2024 budget requests funding for ASPR in a separate, new appropriation account. This table is comparably adjusted to remove ASPR's programs from FY 2022 and FY 2023.

Detail of Positions

Public Health and Social Services Emergency Fund	**FY 2022 Final**	**FY 2023 Enacted**	**FY 2024 President's Budget**
Executive level I	-	-	-
Executive level II	-	-	-
Executive level III	-	-	-
Executive level IV	1	1	1
Executive level V	1	1	1
Subtotal Executive Level Positions	2	2	2
Total - Exec. Level Salaries	**385,550**	**401,754**	**597,063**
ES-6	-	-	-
ES-5	-	-	-
ES-4	-	-	-
ES-3	-	-	-
ES-2	-	-	-
ES-1	-	-	-
Subtotal ES positions	-	-	-
Total - ES Salary	**-**	**-**	**-**
GS-15/CC O-6	26	26	48
GS-14/CC O-5	50	58	86
GS-13/CC O-4	52	70	116
GS-12/CC O-3	24	34	67
GS-11/CC O-2	3	4	32
GS-10	-	-	-
GS-9	4	3	25
GS-8	1	1	1
GS-7	-	-	-
GS-6	-	-	-
GS-5	-	-	-
GS-4	-	-	-
GS-3	-	-	-
GS-2	-	-	-
GS-1	-	-	-
Subtotal	160	196	375
Total - GS Salary	**20,359,760**	**22,635,520**	**53,800,232**
Average ES level	--	--	--
Average ES salary	--	--	--
Average GS grade	13	13	13
Average GS salary	127,248	115,487	143,467
Average Special Pay categories	--	--	--

Note: The Public Health and Social Services Fund previously contained the annual appropriation for the Administration for Strategic Preparedness and Response (ASPR). The FY 2024 budget requests funding for ASPR in a separate, new appropriation account. This table is comparably adjusted to remove ASPR's programs from FY 2022 and FY 2023.

Programs Proposed for Elimination

No programs within the PHSSEF are proposed for elimination.