Office of the Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
Washington, DC 20528

WELCOME TO THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

NEW EMPLOYEE ORIENTATION VIRTUAL AGENDA

Monday

8:00 AM	WELCOME – **Volunteers required** OATH OF OFFICE
8:15 AM	DHS OVERVIEW: HISTORY/CULTURE OF DHS - **Volunteers required** CISA OVERVIEW: HISTORY/CULTURE OF CISA - **Volunteers required**
9:00 AM	ENTERPRISE DATA MANAGEMENT - **Volunteers recommended, not required**
9:15 AM	RECORDS MANAGEMENT - **Volunteers required**
9:30 AM	EMPLOYEE & LABOR RELATIONS – **Volunteers required**
9:45 AM	EXTERNAL AFFAIRS - **Volunteers recommended, not required**
10:00 AM	EEO BRIEFING - **Volunteers recommended, not required**
10:25 AM	BREAK
10:30 AM	COMPLETION OF PERSONNEL/PAYROLL FORMS – **Volunteers required**
11:00 AM	BENEFITS BRIEFING FOR FEDERAL EMPLOYEES/ EAP/WORKLIFE BRIEFING
12:00 PM	LUNCH
12:45 PM	PRIVACY BRIEFING – **Volunteers recommended, not required**
1:00 PM	ETHICS BRIEFING – **Volunteers recommended, not required**
2:00 PM	EMPLOYEE PREPAREDNESS – **Volunteers recommended, not required**
2:30 PM	BREAK
2:45 PM	COUNTERINTELLIGENCE – **Volunteers recommended, not required**
3:15 PM	PROFESSIONAL DEVELOPMENT & TRAINING- **Volunteers not recommended**
3:30 PM	PLANNING, ANALYTICS & SYSTEMS- **Volunteers recommended, not required**
3:45 PM	QUESTIONS & RECAP

Office of the Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
Washington, DC 20528

WELCOME TO THE DEPARTMENT OF HOMELAND SECURITY

NEW EMPLOYEE ORIENTATION VIRTUAL AGENDA

Tuesday

8:00 AM	CISA SECURITY OFFICE AND COMPLIANCE BRIEFING – **Volunteers required**
9:30 AM	ORIENTATION WRAP UP
9:45 AM	**TS/SCI BRIEFING (TS/SCI PERSONNEL ONLY) **

ORIENTATION HOSTS & FACILITATORS:

OCHCO Talent Management Division

Top Secret/SCI Clearance Employees Only

Cybersecurity and Infrastructure Security Agency

On November 16, 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018. This landmark legislation elevates the mission of the former National Protection and Programs Directorate (NPPD) within DHS and establishes the Cybersecurity and Infrastructure Security Agency (CISA).

- CISA leads the national effort to *defend* critical infrastructure against the threats of *today*, while working with partners across all levels of government and in the private sector to *secure* against the evolving risks of *tomorrow*.
- The name CISA brings recognition to the work being done, improving it's ability to engage with partners and stakeholders, and recruit top cybersecurity talent.

What Does CISA Do?

CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

Proactive Cyber Protection:

- CISA's National Cybersecurity and Communications Integration Center (NCCIC) provides 24x7 cyber situational awareness, analysis, incident response and cyber defense capabilities to the Federal government; state, local, tribal and territorial governments; the private sector and international partners.
- CISA provides cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies.

Infrastructure Resilience:

- CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.
- CISA provides consolidated all-hazards risk analysis for U.S. critical infrastructure through the National Risk Management Center.

Emergency Communications:

- CISA enhances public safety interoperable communications at all levels of government, providing training, coordination, tools and guidance to help partners across the country develop their emergency communications capabilities.
- Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters.

Organizational Changes Related to the CISA Act

The CISA Act establishes three divisions in the new agency: Cybersecurity, Infrastructure Security and Emergency Communications.

- The Act transfers the Office of Biometrics Identity Management (OBIM) to DHS's Management Directorate. Placement within the DHS Headquarters supports expanded collaboration and ensures OBIM's capabilities are available across the DHS enterprise and the interagency.
- The bill provides the Secretary of Homeland Security the flexibility to determine an alignment of the Federal Protective Service (FPS) that best supports its critical role of protecting federal employees and securing federal facilities across the nation and territories.

Election Security: #Protect2020

The Cybersecurity and Infrastructure Security Agency (CISA) continues conducting regular vulnerability assessments of election infrastructure and is actively working with state and local election officials every day. The maturation and evolution of our support to the election security community is a clear recognition that election security is, and will be, a top priority for CISA.

#Protect2020

Preach – get out to your communities to raise awareness on security practices, and advocate for broader participation in election security and national security efforts at all levels.

Plan – know what you are going to do in the run up to an election; where you are voting, what the registration laws are in your state, how provisional ballots work, and what you need to do and have in place before, on, and after election day.

Participate – whatever you do, participate in the process whether that is by voting, volunteering, or contributing additional resources. If you are part of the security community, let's push back against the bad guys.

Working with State and Local Officials

CISA continues to prioritize elections, engage our partners, and share information on threats and mitigation tactics as we head towards the 2020 election cycle. CISA's priorities are first and foremost to continue to broaden the reach and depth of information sharing and assistance that CISA provides to state and local election officials.

CISA's primary election security focus in 2018 was at the state and local level, but are helping various political campaigns at the national level as they start popping up in the run up to the 2020 elections.

CISA is currently working with all 50 states and more than 1600 local jurisdictions and is proud of that level of partnership and engagement but recognize we have a lot more work to do. All of the services CISA offers are free, voluntary, protected, and confidential.

Government Coordinating Council and Sector Coordinating Council

CISA will build on the work it has done with the Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) to understand the scope and nature of the risks to elections and have more in depth conversations about some of the harder issues in this sector. Our goals for 2020 include:

- Achieving 100 percent auditability by 2020,
- Improving the efficiency and effectiveness of audits,
- Incentivizing the patching of election systems, AND
- Working with states to develop current and target cybersecurity profiles (utilizing the National Institute of Standards and Technology framework.

THE WAR ON PINEAPPLE: Understanding Foreign Interference in 5 Steps

To date, we have no evidence of Russia (or any nation) actively carrying out information operations against pizza toppings. This infographic is an ILLUSTRATION of how information operations have been carried out in the past to exploit divisions in the United States.

1. TARGETING DIVISIVE ISSUES

Foreign influencers are constantly on the lookout for opportunities to inflame hot button issues in the United States. **They don't do this to win arguments; they want to see us divided.**

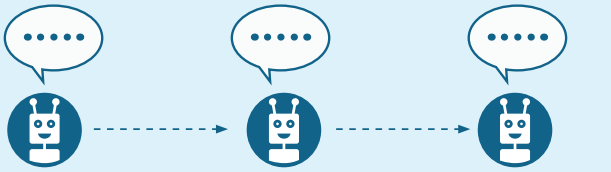
American Opinion is Split: Does Pineapple Belong on Pizza?

An A-list celebrity announced their dislike of pineapples on pizza, prompting a new survey. No matter how you slice it, Americans disagree on the fruit topping.

2. MOVING ACCOUNTS INTO PLACE

Building social media accounts with a large following takes time and resources, so accounts are often renamed and reused. Multiple accounts in a conversation are often controlled by the same user.

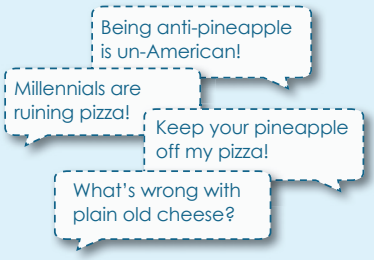
Pro Tip: Look at an account's activity history. **Genuine accounts usually have several interests and post content from a variety of sources.**



3. AMPLIFYING AND DISTORTING THE CONVERSATION

Americans often engage in healthy debate on any number of topics. Foreign influencers try to pollute those debates with bad information and make our positions more extreme by picking fights, or "trolling" people online.

Pro Tip: Trolls try to make people mad, that's it. **If it seems like an account is only aiming to raise tensions, think about whether it's worth engaging.**



4. MAKING THE MAINSTREAM

Foreign influencers "fan the flames" by creating controversy, amplifying the most extreme version of arguments on both sides of an issue. These are shared online as legitimate information sources.

Sometimes controversies make it into the mainstream and create division among Americans. **This is a foreign influencer striking gold! Their meddling is legitimized and carried to larger audiences**.

5. TAKING THE CONVERSATION INTO THE REAL WORLD

In the past, Kremlin agents have organized or funded protests to further stoke divisions among Americans. They create event pages and ask followers to come out.

What started in cyberspace can turn very real, with Americans shouting down Americans because of foreign interference.

Pro Tip: Many social media companies have increased transparency for organization accounts. **Know who is inviting you and why.**

Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
Washington, DC 20528

Biography

Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department Homeland Security

Director Christopher Krebs was sworn in on June 15, 2018 as the Director for the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Krebs was nominated for the position by President Trump in February 2018.

Before serving as CISA Director, Mr. Krebs was appointed in August 2017 as the Assistant Secretary for Infrastructure Protection. In the absence of a permanent NPPD Under Secretary at the time, Mr. Krebs took on the role of serving as the Senior Official Performing the Duties of the Under Secretary for NPPD until he was subsequently nominated as the Under Secretary and confirmed by the Senate the following year.

Mr. Krebs joined DHS in March 2017, first serving as Senior Counselor to the Secretary, where he advised DHS leadership on a range of cybersecurity, critical infrastructure, and national resilience issues. Prior to coming to DHS, he was a member of Microsoft's U.S. Government Affairs team as the Director for Cybersecurity Policy, where he led Microsoft's U.S. policy work on cybersecurity and technology issues.

Before Microsoft, Mr. Krebs advised industry and Federal, State, and local government customers on a range of cybersecurity and risk management issues. This is his second tour working at DHS, previously serving as the Senior Advisor to the Assistant Secretary for Infrastructure Protection and playing a formative role in a number of national and international risk management programs.

As Director, Mr. Krebs oversees CISA's efforts to defend civilian networks, secure federal facilities, manage systemic risk to National critical functions, and work with stakeholders to raise the security baseline of the Nation's cyber and physical infrastructure.

Mr. Krebs holds a bachelor's degree in environmental sciences from the University of Virginia and a J.D. from the Antonin Scalia Law School at George Mason University.

Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
Washington, DC 20528

Biography

Matthew Travis
Deputy Director
Cybersecurity and Infrastructure Security Agency
U.S. Department Homeland Security

Matthew Travis serves as Deputy Director for the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). As Deputy Director, he supports the CISA Director in overseeing the Cybersecurity Division, the Infrastructure Security Division, the Federal Protective Service, the Emergency Communications Division, the Office of Biometric Identity Management and the National Risk Management Center. His operational support responsibilities are to ensure a holistic approach to critical infrastructure protection across physical and cyber risks activities.

Prior to joining CISA in March 2018, Mr. Travis served as vice president of homeland security for Cadmus, a security and resiliency professional services firm supporting clients throughout the homeland security enterprise. In 2010, he co-founded Obsidian Analysis, Inc., a homeland security consultancy. Obsidian was acquired by Cadmus in 2016. In both companies, Mr. Travis served as a senior facilitator of national preparedness exercises in support of FEMA and the National Exercise Program. He also directed all program support for National Level Exercise 2012, the first national cybersecurity exercise.

Previously, Mr. Travis served as president of the information security company Detica, Inc. and, before that, vice president at DFI International, where he was instrumental in creating the homeland security practice that supported NPPD and its Office for Bombing Prevention.

From 1991 to 1998, Mr. Travis served as an officer in the U.S. Navy. He initially served aboard the guided-missile frigate U.S.S. CARR (FFG 52) as the Engineering Auxiliaries Officer. Aboard CARR, he also served as maritime interdiction boarding officer in the Northern Red Sea following Operation DESERT STORM. Mr. Travis then served a tour as White House Liaison to the Secretary of the Navy and was also a White House Military Aide.

Mr. Travis is originally from Terre Haute, Indiana. He is a 1991 graduate of the University of Notre Dame and holds a master's in National Security Studies from Georgetown University.

Preferences Menu

The Preferences menu allows employees to maintain their user ID and password, store two email addresses, and set up challenge questions. User IDs and passwords can be changed at any time. With the ability to store two email addresses in EPP, employees can receive email notifications from NFC and recover lost user IDs and passwords.

Requests for EPP Access

Employees should access the NFC home page on the Internet *(www.nfc.usda.gov)* and select My EPP. To obtain a password, employees should select the signup icon. The password will be mailed directly to the employee by NFC. The NFC-assigned password must be changed by the employee on the first access of the EPP. Employees are encouraged to periodically change this password to ensure confidentiality.

System Requirements

- A personal computer with Internet capabilities
- Access to the Internet with one of the following browsers:
  - Microsoft Internet Explorer Version 6 or higher
  - Netscape
  - Firefox Version 3 or higher
  - Safari
- A browser supporting 128-bit Secure Socket Layer encryption (United States version)

Procedure and Online Help

Additional information on the use of EPP/ESS is available to employees within the EPP Procedure Manual. The EPP procedure can be accessed from the **Publications** link of NFC's Home Page *(www.nfc.usda.gov)*. Online help is also available within EPP itself by selecting the **Help** link on the EPP top navigation menu.

Additional Information

Employees with questions about their EPP should contact their agency personnel office. Agencies needing additional information on the EPP should contact the Client Management staff at:

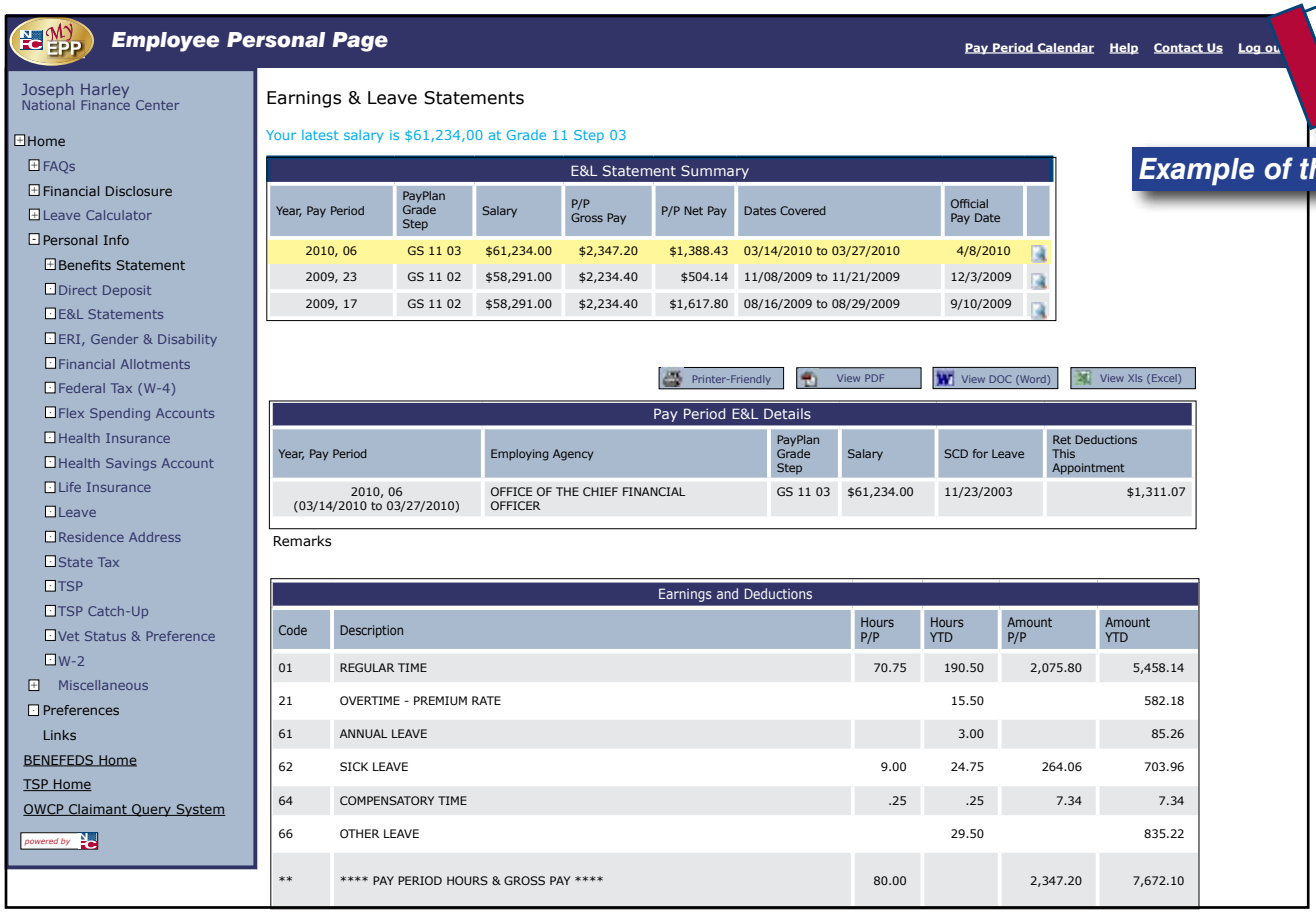
Client Management Branch
National Finance Center, USDA
ATTN: CS-0811
P.O. Box 60000
New Orleans, LA 70160-0001
email: customer.support@usda.gov

NATIONAL FINANCE CENTER
U. S. DEPARTMENT OF AGRICULTURE
NEW ORLEANS, LA

National Finance Center
Office of the Chief Financial Officer
United States Department of Agriculture

Form AD-1129 (Rev. 8/11)

The Employee Personal Page (EPP) allows employees serviced by the National Finance Center (NFC) to view their payroll, leave, health and life insurance, W-2, and other personal information. EPP also allows employees to use a self-service feature to request updates to specific payroll related information.



Example of the Earnings and Leave Statement window

Features

- EPP is convenient, reliable, easy to navigate, and can be accessed 24 hours a day, 7 days a week.
- EPP allows employees to view and change data (by using the Self Service option) without having to submit change requests to their agency personnel office.
- EPP delivers data needed by the employee for income and W-2 verification.

Personal Info Menu

The Personal Info menu provides employees access to their current information for direct deposit, Earnings and Leave Statement, Personal Benefits Statement, financial allotments, Federal tax (W-4), Flexible Spending Accounts, health insurance, Health Savings Account, life insurance, leave, residence address, Federal tax, state tax, Thrift Savings Plan (TSP), Veterans Status/ Preference, and W-2.

Self Service Option

Within the Personal Info menu, employees have the ability to use the self-service feature to make online change requests to their direct deposit, financial allotments, Federal and state tax withholdings, flexible spending accounts, health insurance, residence address, and TSP contributions for current and future pay periods. Employees can also view a history of their previously submitted self-service transactions.

Time Manager (for STAR 5.0 Users)

For agencies using STAR 5.0, the Time Manager option provides employees with the ability to record their daily time and attendance (T&A) data. This functionality also provides employees the ability to establish a default schedule to use as a starting point each pay period.

Each agency must elect to offer its employees the Time Manager daily entry option before they can begin using this feature of EPP. This option is activated at the contact point level.

Leave Calculator

The Leave Calculator provides employees the ability to track leave accruals and usage.

PAY PERIOD CALENDAR 2020

Month	Pay Period	S	M	T	W	T	F	S
JAN	26				1	2	3	4
	01	5	6	7	8	9	10	11
		12	13	14	15	16	17	18
	02	19	20	21	22	23	24	25
		26	27	28	29	30	31	
FEB								1
	03	2	3	4	5	6	7	8
		9	10	11	12	13	14	15
	04	16	17	18	19	20	21	22
		23	24	25	26	27	28	29
MAR	05	1	2	3	4	5	6	7
		8	9	10	11	12	13	14
	06	15	16	17	18	19	20	21
		22	23	24	25	26	27	28
	07	29	30	31				
APR					1	2	3	4
		5	6	7	8	9	10	11
	08	12	13	14	15	16	17	18
		19	20	21	22	23	24	25
	09	26	27	28	29	30		
MAY							1	2
		3	4	5	6	7	8	9
	10	10	11	12	13	14	15	16
		17	18	19	20	21	22	23
	11	24	25	26	27	28	29	30
		31						
JUN			1	2	3	4	5	6
	12	7	8	9	10	11	12	13
		14	15	16	17	18	19	20
	13	21	22	23	24	25	26	27
		28	29	30				

Month	Pay Period	S	M	T	W	T	F	S
JUL	13				1	2	3	4
	14	5	6	7	8	9	10	11
		12	13	14	15	16	17	18
	15	19	20	21	22	23	24	25
		26	27	28	29	30	31	
AUG								1
	16	2	3	4	5	6	7	8
		9	10	11	12	13	14	15
	17	16	17	18	19	20	21	22
		23	24	25	26	27	28	29
	18	30	31					
SEP				1	2	3	4	5
		6	7	8	9	10	11	12
	19	13	14	15	16	17	18	19
		20	21	22	23	24	25	26
	20	27	28	29	30			
OCT						1	2	3
		4	5	6	7	8	9	10
	21	11	12	13	14	15	16	17
		18	19	20	21	22	23	24
	22	25	26	27	28	29	30	31
NOV		1	2	3	4	5	6	7
	23	8	9	10	11	12	13	14
		15	16	17	18	19	20	21
	24	22	23	24	25	26	27	28
		29	30					
DEC				1	2	3	4	5
	25	6	7	8	9	10	11	12
		13	14	15	16	17	18	19
	26	20	21	22	23	24	25	26
		27	28	29	30	31		

FORM NFC-1217 (Revised 7/15)

SALARY TABLE 2020-DCB
INCORPORATING THE 2.6% GENERAL SCHEDULE INCREASE AND A LOCALITY PAYMENT OF 30.48%
FOR THE LOCALITY PAY AREA OF WASHINGTON-BALTIMORE-ARLINGTON, DC-MD-VA-WV-PA
TOTAL INCREASE: 3.52%
EFFECTIVE JANUARY 2020

Annual Rates by Grade and Step

Grade	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8	Step 9	Step 10
1	$ 25,500	$ 26,354	$ 27,202	$ 28,045	$ 28,893	$ 29,389	$ 30,227	$ 31,073	$ 31,106	$ 31,900
2	28,672	29,354	30,304	31,106	31,456	32,381	33,306	34,231	35,157	36,082
3	31,284	32,326	33,369	34,411	35,454	36,497	37,539	38,582	39,624	40,667
4	35,119	36,289	37,460	38,630	39,800	40,971	42,141	43,312	44,482	45,652
5	39,291	40,601	41,911	43,222	44,532	45,842	47,152	48,462	49,772	51,082
6	43,798	45,258	46,718	48,178	49,639	51,099	52,559	54,019	55,479	56,939
7	48,670	50,292	51,914	53,536	55,158	56,780	58,402	60,023	61,645	63,267
8	53,901	55,698	57,495	59,291	61,088	62,885	64,682	66,478	68,275	70,072
9	59,534	61,519	63,503	65,488	67,473	69,457	71,442	73,426	75,411	77,396
10	65,561	67,747	69,932	72,118	74,303	76,489	78,674	80,860	83,045	85,231
11	72,030	74,431	76,832	79,233	81,634	84,034	86,435	88,836	91,237	93,638
12	86,335	89,213	92,091	94,970	97,848	100,727	103,605	106,483	109,362	112,240
13	102,663	106,085	109,508	112,930	116,353	119,775	123,198	126,620	130,043	133,465
14	121,316	125,360	129,404	133,447	137,491	141,534	145,578	149,621	153,665	157,709
15	142,701	147,458	152,215	156,973	161,730	166,487	170,800 *	170,800 *	170,800 *	170,800 *

* Rate limited to the rate for level IV of the Executive Schedule (5 U.S.C. 5304 (g)(1)).

Applicable locations are shown on the 2020 Locality Pay Area Definitions page: http://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2020/locality-pay-area-definitions/

DHS Rules of Behavior
General Rules of Behavior

- Rules of Behavior that apply to access and use of Department of Homeland Security (DHS)information technology (IT) equipment and systems are a vital part of the DHS IT Security Program and help to ensure the security of systems and the confidentiality, integrity, and availability of sensitive information.
- The purpose of DHS Rules of Behavior is to inform users of their responsibilities and let them know they will be held accountable for their actions while they are accessing DHS systems and using DHS IT resources (including workstations, laptop computers, mobile computing devices, cell phones, smartphones, tablets, removable media such as CDs, DVDs, and both mechanical and solid state portable memory drives) capable of accessing, storing, receiving, or transmitting sensitive information. The DHS Rules of Behavior apply to every DHS employee, DHS support contractor, or others working on behalf of DHS (i.e. employees, detailees, military)
- Users should have no expectation of privacy while using any DHS equipment and while using DHS Internet or email services.
- The baseline Rules of Behavior are consistent with the IT security policy and procedures given by DHS Management Directive 140-1, "Information Technology Systems Security", "DHS Sensitive Systems Policy Directive 4300A," and the "DHS 4300A Sensitive Systems Handbook."
- Where users are not subject to Component-specific rule(s) of behavior, they must comply with those published by the Department.
- The Rules of Behavior apply to users at their primary workplace, at any alternative workplaces, (e.g. teleworking from home or from a satellite site), and while on official travel.
- Any user not in compliance with applicable Rules of Behavior is subject to sanctions that may include verbal or written warning, denial of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, or termination, depending on the severity of the violation.

System Access

- I understand that I am giving access only to those systems to which I require access in the performance of my official duties.
- I will not attempt to access systems I am not authorized to access.

Software

- I agree to abide by software copyrights and to comply with the terms of all licenses.
- I will not install on DHS equipment any unauthorized software, including software available for downloading from the Internet, software available on DHS networks, and personally owned software.

Passwords and Other Access Control Measures

- I understand that DHS has a goal of 100% strong identity authentication that will require use of my Personal Identity Verification card and Personal Identification Number (PIN).
- In those instances where a password must be used, I will use a password that complies with the appropriate Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) as specified by the system Information Systems Security Officer (ISSO).
- I will protect passwords and PINs from disclosure.
- I will not share passwords.
- I will not provide my password to anyone, including system administrators.
- I will not record passwords or PINs on paper or in electronic form.
- To prevent others from obtaining my password via "shoulder surfing," I will shield my keyboard from view as I enter my password.
- I will ensure that my Personal Identity Verification (PIV) card is always in my personal possession.
- I will not store my PIV card with DHS workstations, laptop computers, or mobile computing devices.

- I will promptly change a password or PIN whenever the compromise of that password or PIN is known or suspected.
- I will not attempt to bypass access control measures.

Data Protection

- I will use only DHS equipment or DHS authorized and approved services, such as Workplace as a Service (WPaaS), to access DHS systems and information.
- I will protect sensitive information from disclosure to unauthorized persons or groups.
- I will log off and lock my workstation or laptop computer by removing my PIV card or other secondary authentication device, or I will use a password-protected screensaver, whenever I am away from my work area, even for a short time.
- I will not access, process, or store classified information on DHS office equipment unless use of the equipment is authorized for classified information of the appropriate level.

Use of Government Office Equipment

- I will comply with DHS policy regarding personal use of DHS office equipment. I understand that DHS office equipment is to be used for official use, with only limited personal use allowed. Personal use of Government office equipment is described in DHS Management Directive (MD) 4600, (Personal Use of Government Office Equipment).
- I understand that my use of DHS office equipment may be monitored, and I consent to this monitoring.
- I understand that only content managers designated by the Office of Public Affairs (OPA)may post material to Department and Component Internet sites.
- I understand that personal Internet activities which inhibit the security of DHS information and information systems, or cause degradation of network services are prohibited. Examples of such activity include streaming of audio or video, social networking, peer-to-peer networking, software or music piracy, online gaming, webmail, Instant Messaging (IM), and hacking.
- I understand that the use of webmail or other personal email accounts is prohibited on DHS information systems.
- I understand that the viewing of pornographic or other offensive content is strictly prohibited on DHS furnished equipment and networks

Internet and Email Use

- I understand that I can only use Government systems for official Internet activities and email, with limited personal use allowed. Allowed personal use is described in DHS Directive 142-03, “Electronic Mail Usage and Maintenance” and DHS Directive 262-04, “DHS Web (Internet and Extranet Information).”
- I will not use Government systems for access to webmail.
- I understand that my Internet and email use may be monitored, and I consent to such monitoring.

- I will not use peer-to-peer (P2P) file sharing to connect remotely to other systems for the purpose of sharing files. I understand that P2P can be a means of spreading viruses over DHS networks and may put sensitive government information at risk. I also understand that DHS Sensitive Systems Policy Directive 4300A prohibits the use of P2P software on any DHS-controlled or DHS-operated system.
- I will not provide personal or official DHS information if solicited by email. If I receive an email message from any source requesting personal information or asking to verify accounts or security settings, I will not respond nor open any link therein, but will forward such questionable email to DHSSPAM@hq.dhs.gov and take no other action.

Teleworking

Employees approved for teleworking at any alternative workplace must adhere to the following Rules of Behavior:

- At my alternate workplace, I will follow security practices that are the same as or equivalent to those required of me at my primary workplace.
- I will physically protect any communications and mobile computing devices I use for teleworking when they are not in use.
- I will protect sensitive data at my alternate workplace. This includes properly disposing of sensitive information by shredding or other appropriate means.

Laptop Computers and Portable Electronic Devices

Use of DHS communications and computing devices is subject to following additional rules of behavior:

- I will always keep GFE under my physical control, or I will secure it in a suitable locked container under my control.
- I will password-protect any communications and computing devices I use. I will set the security time out for any communications and mobile computing devices to the established timeout period. For Government Furnished Equipment (GFE) communications and mobile computing devices, the timeout period is 15 minutes.
- When contacted by technical support personnel who request actions on my part, I will verify their authenticity by calling the Help Desk. When I have verified the caller's identity, I will call them as instructed by the Help Desk, and immediately comply with instructions from the technical support personnel to perform update actions, or to make equipment assigned to me available to technical support personnel for updating.
- I will use only DHS-authorized Internet connections that conform to DHS security and communications standards.
- I will take all necessary precautions to protect GFE against loss, theft, damage, abuse, and unauthorized use by employing lockable cases and keyboards, locking cables, and removable storage devices.
- I will use only DHS communications and mobile computing devices to access DHS systems and information.
- I will not make any changes to any GFE system configuration unless I am directed to do so by a DHS system administrator.
- I will not program the laptop with sign-on sequences, passwords, or access phone numbers.
- I understand and will comply with the requirement that sensitive information stored on any laptop computer, used in a residence or on travel, shall be protected using encryption validated in accordance with FIPS 140-2, "Security Requirements for Cryptographic Modules."
- I understand and will comply with the requirement that sensitive information processed, stored, or transmitted on mobile devices must be encrypted using approved encryption methods.

Tips for traveling with a Laptop or other Mobile computing devices

- Keep the laptop or mobile computing device under your physical control at all times.
- At airport security, place the laptop or mobile computing device on the conveyor belt only after the belongings of the person ahead of you have cleared the scanner. If you are delayed, keep your eye on the laptop or mobile computing device until you can pick it up.
- Do not place the laptop or mobile computing device in checked luggage.
- Do not store the laptop or mobile computing device in an airport, a train or bus station, or any public locker.
- If you must leave a laptop or mobile computing device in a car, lock it in the trunk so that it is out of sight.

- Avoid leaving the laptop or mobile computing device in a hotel room. If you must leave it in a hotel room, lock it inside another piece of luggage or in the safe in the hotel room.

Incident Reporting

- I will promptly report IT security incidents in accordance with DHS CISO procedures for detecting, reporting, and responding to information security incidents in accordance with DHS 4300A Sensitive Systems Handbook Attachment F, "Incident Response."

Accountability

- I understand that I have no expectation of privacy while using any DHS equipment and while using DHS Internet or email services.
- I understand that I will be held accountable for my actions while accessing and using DHS systems and IT resources.

ACKNOWLEDGEMENT STATEMENT

I acknowledge that I understand, have read, and will comply with the DHS Rules of Behavior in addition to the following:

- When accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network and (4) all device sand storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use or access of this system may result in disciplinary action, as well as civil and criminal penalties.

By using DHS information system(s), I understand and consent to the following:

- I have no reasonable expectation of privacy when I use this information system; this includes any communications or data transmitting, stored on, originated from or directed to this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, search and seize any communication or data transiting, stored on, originated from or directed to or from this information system.
- The government may disclose or use any communications or data transiting, stored on, originated from or directed to or from this information system for any lawful government purpose.
- I am NOT authorized to process classified information on a non-classified information system.

I understand that failure to comply with the course content including the Rules of Behavior, could result in one or more of the following actions: verbal or written warning; removal of system access; reassignment to other duties; criminal or civil prosecution; termination.

By signing below, I am acknowledging that I understand and have read the Rules of behavior and will comply with its requirements.

Name of User (printed): _____

User's Phone Number: _____

User's Email Address: _____

DHS Component: _____

Location or Address: _____

Supervisor's Name: _____

Supervisor's Phone Number: _____

_____ _____

User's Signature Date

Cybersecurity and Infrastructure Security Agency
New Employee Onboarding Survey

OVERVIEW

This New Employee Onboarding Survey was designed to collect standardized data on different aspects of the Cybersecurity and Infrastructure Security Agency's (CISA) recruiting, hiring, and onboarding processes. Data collected through this survey is used to evaluate and assess the effectiveness of these processes, with the aim of continuously improving the CISA new employee experience.

Any references in the questions below to an "agency" are intended to reflect the Cybersecurity and Infrastructure Security Agency (CISA) as an independent organizational entity rather than the broader Department of Homeland Security or the individual subcomponents or offices within CISA. When answering questions that reference an "agency", please consider your response in the content of CISA.

Please write your primary work location:

Division (Circle One): ☐ **CSD** ☐ **ISD** ☐ **NRMC** ☐ **OD** ☐ **ECD**

Career Level (Circle One): ☐ **Intern/Student** ☐ **Entry Level (GS-9 or GS-11)**

☐ **Mid-Level (GS-12/13)** ☐ **Senior Level (GS-14/15)** ☐ **SES**

Name (Optional):

HIRING PROCESS

1. The job opportunity announcement was clear and understandable (If not, please explain why). ☐ **Yes** ☐ **No**

2. Did you receive a status update regarding your application for the following four touch points?

   A. Application/resume was received ☐ **Yes** ☐ **No**

   B. Application/resume was assessed ☐ **Yes** ☐ **No**

   C. Application/resume was referred ☐ **Yes** ☐ **No**

   D. Notification that a selection was made ☐ **Yes** ☐ **No**

HIRING PROCESS (CONTINUED)

	Did Not Meet Expectations	Met Expectations	Exceeded Expectations
3. The agency interviewer's professionalism about the agency and its mission	☐	☐	☐
4. The human capital contacts were knowledgeable during the hiring process	☐	☐	☐
5. The length of time between when I submitted my application and when I first heard from the agency	☐	☐	☐
6. The length of time between the submission of my application and when I received a Tentative Job Offer (TJO)	☐	☐	☐
7. The ability to identify my role within the agency based on the information provided	☐	☐	☐

BRANDING

	Did Not Meet Expectations	Met Expectations	Exceeded Expectations
8. The representation of the agency's branding throughout the hiring process (i.e. divisions)	☐	☐	☐

AGENCY WEBSITE

	Did Not Meet Expectations	Met Expectations	Exceeded Expectations
9. The ease of use on the agency website (Skip if this was not used)	☐	☐	☐
10. The knowledge presented on:			
A. USAJOBS	☐	☐	☐
B. Electronic Questionnaires for Investigations Processing (E-QIP)	☐	☐	☐
C. USAStaffing (Onboarding Documentation Website)	☐	☐	☐

AFTER YOU ACCEPTED, BUT BEFORE YOUR FIRST DAY ON THE JOB

	Did Not Meet Expectations	Met Expectations	Exceeded Expectations
11. The support and information I received before my first day on the job	☐	☐	☐
12. The Final Job Offer's (FJO) accuracy regarding relevant information	☐	☐	☐
13. The effort the point of contact made to make me feel welcome before starting	☐	☐	☐
14. The willingness to help presented by the point of contact	☐	☐	☐

YOUR FIRST DAY ON THE JOB

15. In the orientation session, clear information was provided about:

A. Agency mission ☐**Yes** ☐**No**

B. The role the agency plays in the Federal government ☐**Yes** ☐**No**

C. Agency organizational structure ☐**Yes** ☐**No**

D. How I will contribute to the accomplishment of the agency's mission.
☐**Yes** ☐**No**

	Did Not Meet Expectations	Met Expectations	Exceeded Expectations
16. The information I received about:			
A. Enterprise Data Management	☐	☐	☐
B. Records Management	☐	☐	☐
C. Employee & Labor Relations	☐	☐	☐
D. External Affairs	☐	☐	☐
E. Equal Employment Opportunity (EEO)	☐	☐	☐
F. Benefits	☐	☐	☐
G. Privacy	☐	☐	☐
H. Ethics	☐	☐	☐
I. Employee Preparedness	☐	☐	☐
J. Counterintelligence	☐	☐	☐
K. Professional Development & Training	☐	☐	☐
L. Policy, Accountability and Systems	☐	☐	☐
M. Security & Compliance	☐	☐	☐

Please provide any comments or questions about the above briefings (timeliness, conciseness or clarity):

17. The information related to where to go to get additional assistance on personnel matters, benefits, and paperwork following my first day on the job	☐	☐	☐
18. Review of Human Capital paperwork	☐	☐	☐
19. Support from Human Capital	☐	☐	☐

20. I believe the job is a good fit for me ☐**Yes** ☐**No**

21. I was attracted to this position by a Federal recruitment effort (e.g. hiring fair) **NOTE**: If you learned about this position from using USAJOBs, please select "No" as your answer. ☐**Yes** ☐**No**

21a. If answered yes from above, how did you learn about this position? (Select 1 below)

- ○ **1.** Internal selection
- ○ **2.** Referred by a current employee
- ○ **3.** LinkedIn or social media
- ○ **4.** Recruiting fair or event: (Please list title of event)_____
- ○ **5.** Other:_____

22. What was your motivation for choosing or accepting this position?

23. Were you aware of CISA's mission/function prior to learning of and applying for the position?
☐**Yes** ☐**No**

23a. If answered yes from above, how did you learn about this position? (Select 1 below)

- ○ **1.** Previously worked for DHS or CISA
- ○ **2.** Federal employee outside of DHS that worked with CISA as part of mission and duties
- ○ **3.** LinkedIn or social media
- ○ **4.** Worked with CISA as a contractor
- ○ **5.** Own research through USAJOBS
- ○ **6.** Other: _____

24. What should be our top priority for improving our onboarding process?

25. Please share any additional feedback or recommendations you may have to improve the agency's hiring and orientation processes.