U.S. Department of Justice
Civil Rights Division

KK:ANF:DKH
20-00265-F
(DOJ-20-2337)

Freedom of Information/PA Unit – 4CON
950 Pennsylvania Ave., NW
Washington, DC 20530

Via Electronic Mail Only
Mr. Austin Evers
1030 15th Street, N.W.
Washington, DC 20005
foia@americanoversight.org

October 7, 2022

Dear Mr. Evers:

This is in further response to your September 22, 2020 Freedom of Information Act request, received by the Civil Rights Division, seeking access to the following records:

> Any final assessments or analyses regarding the projected or actual impacts (such as the impact on the volume of reported violations, whether any class of complaints would be submitted more or less frequently as a result of the new system, or whether a centralized review process would be implemented for complaint processing of consolidating the Civil Rights Division's legacy intake processes and systems for civil rights violation reports into the single Civil Rights Reporting Portal, available at civilrights.justice.gov from January 1, 2019 to the present.

After review of the responsive Civil Rights Division documents, I have determined that the documents may be released to you subject to the excision of the names and other identifying information of private citizens, pursuant to 5 U.S.C. § 552 (b)(6) since disclosure thereof could reasonably be expected to constitute an unwarranted invasion of personal privacy and pursuant to 5 U.S.C. § 552 (b)(5) since the intra-agency memoranda consist of attorney work-product and predecisional deliberative material. Please be advised that we have considered the foreseeable harm standard when reviewing records and applying FOIA exemptions.

Enclosed are Civil Rights Division of responsive documents.

If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, DC 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following web site: https://www.justice.gov/oip/submit-and-track-request-or-appeal. Your appeal must be

postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

I hope the Civil Rights Division has been of some assistance to you in this matter.

Sincerely,

Kilian Kagle

Kilian Kagle, Chief
Freedom of Information/Privacy Acts Unit
Civil Rights Division

Civil Rights Division

Privacy Impact Assessment
for the
Civil Rights Violations Reporting Portal

Issued by:
Michelle Ramsden

Approved by: Erika Brown Lee, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: October 11, 2019

(May 2015 DOJ PIA Template)

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the system.

EXECUTIVE SUMMARY

The Civil Rights Division (CRT) intends to modernize how it intakes reports of civil rights violations from the public. To do so, CRT is developing a web-based reporting platform to report violations of federal civil rights laws (Portal).

CRT is conducting a privacy impact assessment because the Portal will allow members of the public to provide CRT with their contact information (name, email, phone, etc.). Moreover, because the Portal will allow members of the public to describe what they witnessed, it may capture sensitive volunteered information.

Section 1: Description of the Information System

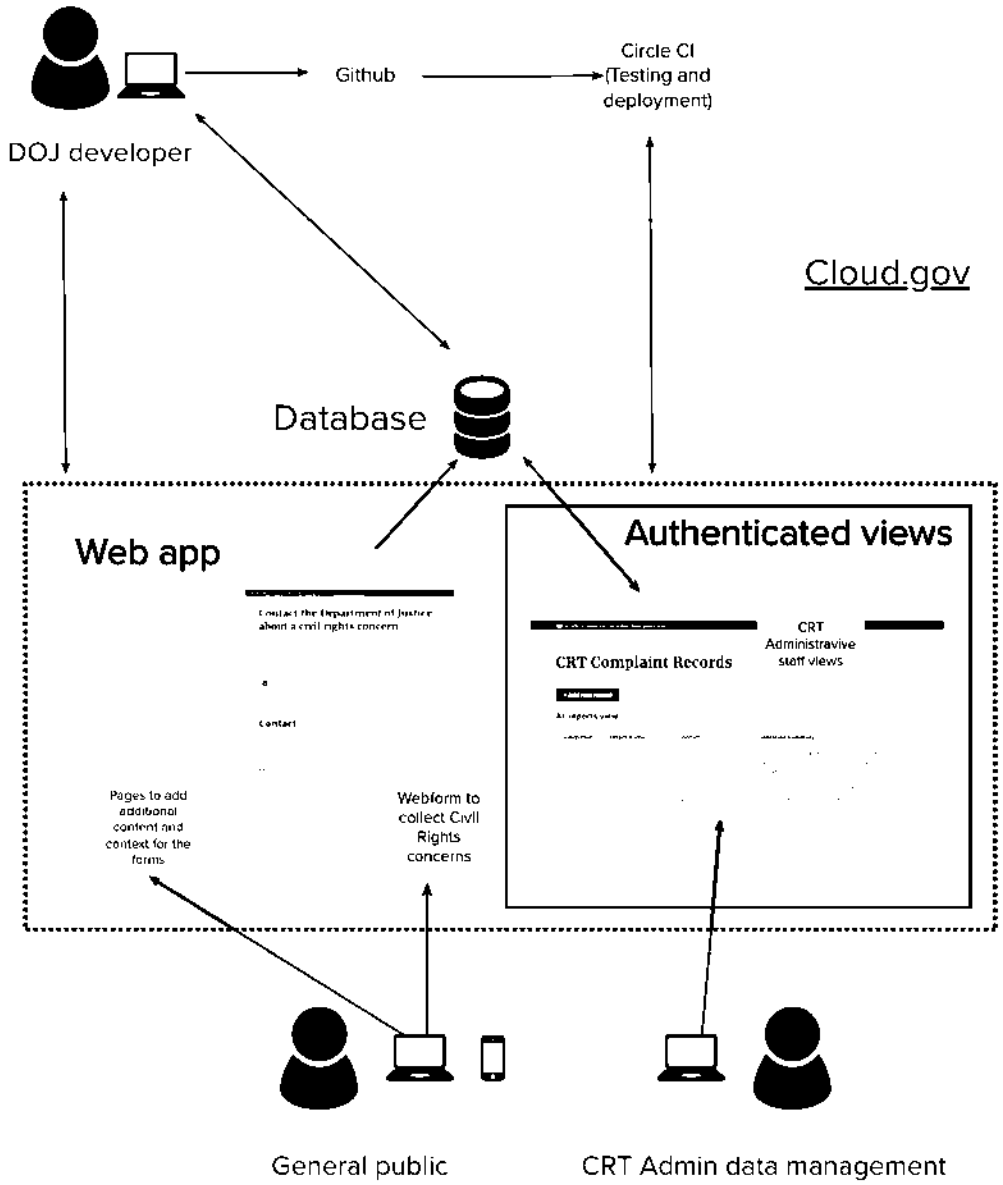
Purpose of the Records & the System

CRT developed the Portal with two primary goals. To:

- Create a clearer, more seamless experience for members of the public who report violations of federal civil rights laws to CRT, and
- Ease the burden on CRT staff CRT's employees currently intake complaints through highly varied and often manual means – the Portal will automate and otherwise reduce steps in processing.

How the System Operates

The System consists of web app and database designed to achieve the purpose described above. See descriptions of the diagram components below.



- **Web app** – members of the public who want to report a potential civil rights violation

online would visit the CRT web form. On that page, the public would be able to access a streamlined, responsive web form to report potential violations of federal civil rights laws. Upon submission of the data, the form responses will be sanitized to prevent SQL injection before it reaches the database. The web app is a Python/Django application. We will set up two or more instances of the app to ensure availability.

- **Authenticated views for the web app** – CRT employees responsible for intaking public violations will access the database using a password-protected, cloud-based interface that will allow them to search, sort, re-route, and review the reports provided by the public. This internal interface will also allow intake specialists to add reports to the System that they receive through non-web channels, such as mail, telephone, email, etc. To protect the confidentiality of the data, we will integrate with the DOJ's single sign on, so that all authenticated views are compliant with DOJ account policy and provide PIV sign on.

- **Database** – the data collected by the web app and seen in the internal interface is stored and managed in a secure database. When the public provides information through the webform, CRT will store the information in a database on a secure cloud-based server. This Postgres database will be encrypted at rest. The database is set up for automatic backups. For production we will also be setting up a redundant database instance. Developers also have access to the system via cloud.gov, but would only need to connect in rare circumstances.

- **Cloud.gov** these aforementioned components are hosted in Cloud.gov, which is a PaaS that provides the infrastructure, operating system, and supporting technologies required to run the app. Cloud.gov has a FedRAMP Moderate authorization and is built on AWS GovCloud. AWS GovCloud regions are operated by employees who are U.S. citizens on U.S. soil. We would also like to integrate DOJ's single sign on, with developer access to cloud.gov so that they can use their PIVs to log in and access can be centrally managed by DOJ. There will be a long drain service so that logs feed into DOJ's central Splunk system. (See security documentation and the FedRAMP package for more details.)

- **Testing and deployment tools-** GitHub and CircleCI are part of the automated testing and deployment infrastructure to help ensure the quality and security of the application. Static code analysis is run on every code change to flag potential security vulnerabilities. Automated deploys with allow for deploys of the application without downtime, increasing the availability of the system. Automated tests are run on every code change to ensure that endpoints that not public are protected by authentication. GitHub houses the codebase and also checks that application level dependencies are up to date.

CRT is developing these components to work together to accomplish the goals above.

Types of Information Collected

Using the System, members of the public can provide the following kinds of information to CRT:

- His/her/their contact information (name, address, phone, email)
- Information about the witnessed violation, including the witness's belief about:
    - Why the discrimination occurred (i.e., protected class),
    - When the discrimination occurred,
    - Where the discrimination occurred,
    - Who allegedly committed a discriminatory act, including location details (city, state, zip code, name of person or organization), and
    - A description of what happened, in the witness's own words.

Who Has Access to the System

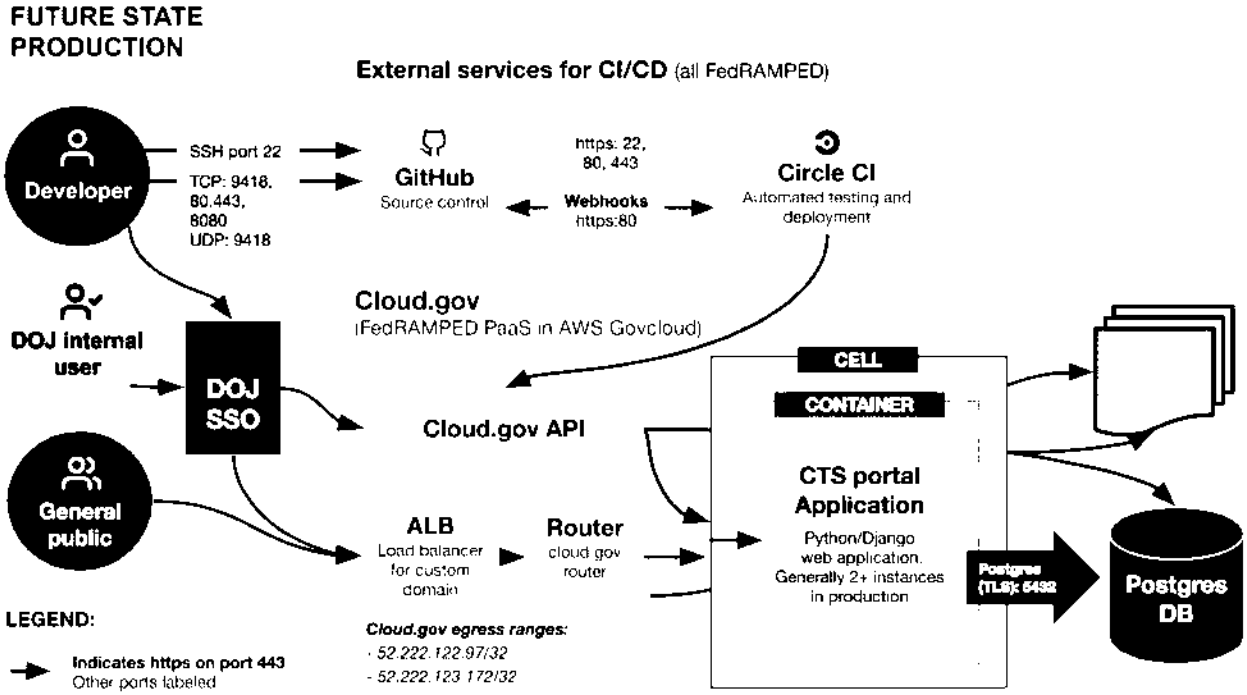
- **Members of the public**
    - The public will be able to access certain parts of the web application which are public-facing, including the homepage and the complaint form. These pages will be available to any member of the public using any web browser. Members of the public will be able to submit complaints to the Civil Rights Division by using the form.
    - Members of the public will ***not*** have the ability to read the reports left by others. Pages designed for CRT use only will be guarded from members of the public by our application's authorization and authentication logic, which will be tested by our automated test suite.
- **Intake specialists with the Civil Rights Division** –
    - Through our application's internal interface, intake specialists will have access to the data provided by the public. This will take the form of a "view all" table collating complaints from the public. Intake specialists will have permissions to add new reports, view reports, comment on reports, and update the status of reports. Intake specialists will not be able to delete or edit the content of what was reported by the public. These permissions will be enforced by the authorization and authentication logic of our Django application, which will be tested by our automated test suite.
- **Administrators**
    - One to two administrators on CRT's information technology and/or correspondence teams will have full access to the System. Administrators will have access in order to facilitate the intake process where needed, and to administer and improve the System. These users will have access to the Django administration backend which provides users with full control over the data, including the ability to add, view, update and delete records.
- **Developers** -
    - CRT developers will have access to the code and data in order to create, maintain, debug and enhance the system. They will be able to log into the application's Postgres database directly, propose changes to the source code, inspect logs, and administer the application's Cloud.gov infrastructure.

How Users Retrieve Information in the System

- **Members of the public** – will not be able to retrieve information from the System.
- **Intake specialists** - will have access to an internal-facing interface provided by authenticated views that display the relevant reports provided by the public. This interface will allow intake specialists to search, sort, re-route, and review the reports using a table format. This staff will be able to use criteria such as filed date, type of report, and any public-provided data to find any report.
- **Administrators** - will have direct access to the database, as well as to the internal interface. All administrative actions that affect the data will be logged. Those logs will be available to DOJ SOC by sending the logs to their Splunk instance.

How Information is Transmitted to and From the System

Network diagram:



Web app

- Members of the public will transmit information through a webform. The public will be able to visit the webform using any browser, and input information about their complaint using our 508 compliant, step-by-step webform. This webform will only accept encrypted https connections to protect the public's data while in transit on any network.
- DNS will direct the traffic to an Application Load Balancer (ALB) in Cloud.gov. The ALB then goes to a Cloud.gov Router that traffic is then directed to an instance of the app via the app's cell and container.

- Upon submission of the data, the form responses will be sanitized to prevent SQL injection and then flow into the Postgres database associated with our application.
- Information will be transmitted from the system to intake specialists in the application's authenticated views. Intake specialist will only be able to see those views, if authorized by the system and they log in using the DOJ's SAML integration. Once a specialist is logged in, they will then be able to view complaint information collated into a table and query that data. All traffic will be encrypted with HTTPS.
- Information will also be transmitted to the system in some authenticated views when administrators log on and leave comments on the form entries or when using the Django administrator backend to manually add a complaint record to the system. For example, to record information from the public received by phone. These views will have the same measures as the authenticated views.
- Logs created by the web app are automatically captured in Cloud.gov and we will set up a log drain service to feed into DOJ's Splunk instance.
- Static assets for the app are stored in Cloud.gov's AWS Simple Storage Service (S3). These are publicly available assets such as javascript, css and image files for the web app. These assets are created by the application as part of the deploy process.

Postgres Database

- The database receives connections using the Transport Layer Security (TLS) protocol. That ensures all connections are encrypted.
- Developers can create a service key for the database, using the Cloud.gov API and connect via TLS, but this should be done only sparingly.
- Logs created by the database are automatically captured in Cloud.gov and we will set up a log drain service to feed into DOJ's Splunk instance.

*Note that Circle CI triggers the deploy by pushing code with start up commands that run in cloud.gov but it does not have direct access to the data.

Interconnectedness of the System

This System is a standalone. However, future development of the System may allow users to export data to CRT's Correspondence Tracking System and Interactive Case Management System.

Type of System

This System is listed as a major application.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated.

(Check all that apply.)

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):					

General personal data					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address	X	Medical information	
Gender		Telephone number	X	Military service	
Age		Email address	X	Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify): In addition to the types of personal data identified above, it is possible that - as members of the public describe the alleged discrimination they witnessed they will include narrative responses indicating their Gender, Race/Ethnicity, Place of Birth, Education, Religion, Military Service, and Physical Characteristics.					

Work-related data					
Occupation		Telephone number	X	Salary	
Job title		Email address	X	Work history	
Work address		Business associates			
Other work-related data (specify): It is possible that - as members of the public describe the alleged discrimination they witnessed they will include narrative responses that include additional work-related data.					

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	

Other distinguishing features/biometrics (specify):

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	
IP address	X	Queries run	X	Contents of files	
Other system/audit data (specify): Per JMD System Event logs, DB & Web logs, PowerShell logs, DNS logs,					

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government sources					
Within the Component		Other DOJ components		Other federal entities	
State, local, tribal		Foreign			
Other (specify):					

Non-government sources					
Members of the public	X	Public media, internet		Private sector	
Commercial data brokers					
Other (specify):					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the

information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

CRT limited and tailored the Portal to collect the information that is necessary to:

- More accurately route reports of civil rights violations to the CRT section most likely to cover the subject matter of the complaint, and
- Give CRT intake specialists with the information needed to evaluate and determine how best to handle any report of a civil rights violation.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities	X	For civil enforcement activities
	For intelligence activities		For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
X	For litigation		
	Other (specify):		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

- Civil enforcement activities CRT's various civil enforcement sections will review and assess reports of violations from the Portal. Where appropriate and authorized by law, these sections may use reports from the Portal to initiate a new investigation or add to an ongoing investigation or case.
- Litigation – if CRT receives a report of a civil rights violation through the Portal that relates to on-going litigation, CRT may use this information in that on-going litigation.
- Criminal law enforcement – the Portal will generally direct individuals who are victims/ witnesses of potentially criminal conduct to contact the FBI or other law enforcement. However, it is possible that civil enforcement sections of CRT may review reports from the Portal and later identify potential criminal violations. In that case, these civil litigating sections may refer such reports to CRT's Criminal Section for review.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	• Official Misconduct, 18 U.S.C. §§ 241, 242 • The Matthew Shepard and James Byrd, Jr., Hate Crimes Prevention Act of 2009 • Federally Protected Activities, 18 U.S.C. § 245 • Criminal Interference with Right to Fair Housing, 18 U.S.C. § 3631 • Damage to Religious Property, 18 U.S.C. § 247 • Trafficking Victims Protection Act (TVPA) • Freedom of Access to Clinics Entrances Act (FACE) • Criminal Protection for Voting Rights, 18 U.S.C. § 594 • Americans with Disabilities Act, Title I • Americans with Disabilities Act, Title II • Americans with Disabilities Act, Title III • Rehabilitation Act of 1973 • Civil Rights Act of 1964, Title VII • Uniformed Services Employment and Reemployment Rights Act (USERRA) • Civil Rights Act of 1964, Title IV • Equal Education Opportunities Act of 1974 (EEOA) • Individuals with Disabilities in Education Act (IDEA) • Civil Rights Act of 1964, Title VI • Education Amendments of 1972, Title IX • Civil Rights Act of 1964, Title II • Fair Housing Act (FHA) • Equal Credit Opportunity Act (ECOA) • Religious Land Use and Institutionalized Persons Act (RLUIPA) • Servicemembers Civil Relief Act (SCRA) • Immigration and Nationality Act § 274B • Civil Rights of Institutionalized Persons Act (CRIPA) • Violent Crime Control and Law Enforcement Act § 14141 • Omnibus Crime and Safe Streets Act • Voting Rights Act • Voting Accessibility for the Elderly and Handicapped Act • Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) • National Voter Registration Act (NVRA) • Genetic Information Nondiscrimination Act (GINA), Title II • Help America Vote Act (HAVA) • Civil Rights Acts of 1870, 1957, 1960, & 1964
	Executive Order	
	Federal Regulation	
	Memorandum of Understanding/agreement	
	Other (summarize and	

	provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

I. Incoming Complaints and Correspondence (received by mail, email, fax, phone or website)

A. Does the topic potentially fall within CRT's purview for action?

1. Yes Proceed to II.
2. No – Determine Appropriate Referral:

a) **Referral to Another DOJ Component (excluding FBI)** Send original electronic correspondence to appropriate component with no CRT written response to the incoming correspondence. No incoming material is retained by CRT.

b) **Discretionary Referral to Non-DOJ Agencies without Administrative Filing Deadlines** - Send original electronic correspondence with referral letter to appropriate agency. Send a form letter response indicating the referral. Retain the record in the online portal for 1 year after cutoff[1] and then destroy. DAA-0060-2014-0004-0001.

c) **Nondiscretionary Referral to the FBI and Agencies with Administrative Filing Deadline** (FBI, HUD, DOL/VETS, DoEd/OCR, and EEOC) Send original electronic correspondence with referral letter to appropriate agency. Send a form letter response indicating the referral. Retain the record (an electronic copy of the incoming and our referral) in the online portal for 3 years after cutoff and then destroy. DAA-0060-2014-0004-0002.

d) **Follow up letters after referral** – Send form response with a copy of the prior CRT form letter indicating the referral. No need to respond if the content of additional incoming letters received from the same sender do not fall within CRT's purview. Refer any complainant writing in for copies of their complaint and/or attachments (CRT website advises to send copies and not originals) to the FOI/PA Branch. (Retain mail and attachments 1 year after cutoff and then destroy).

[1] The "cutoff" referred to throughout this document is the end of the calendar year in which the correspondence was received.

e) **Unsure where to refer the correspondence** – Send original electronic correspondence via ~~interoffice~~ electronic mail to the DOJ Mail Referral Unit (askdoj@usdoj.gov) for reassignment. No material is retained by CRT.

II. Determine whether a CRT response is needed:

A. **No response is needed when the incoming correspondence falls within the following categories**:

1. Write-in campaign;
2. Personal opinion on current events or personal experiences;
3. Informational or reference literature;
4. Routine complaints, commendations or other correspondence (deemed non-substantive material and the response would amount to an acknowledgement of receipt);
5. Anonymous communications, such as suggestion box comments;
6. Public correspondence received in error or addressed to another entity and copied to DOJ; or
7. Repeat writers (*3 or more contacts about the same subject or allegations without additional meaningful information or support to warrant CRT action*).

B. If no response is needed, retain an electronic copy of incoming information for 1 year from cutoff in the online portal, then schedule destruction. DAA-0060-2014-0004-0001

C. If the incoming correspondence does not fall within the above categories, proceed to III.

III. Classify the correspondence to determine next action:

A. **A response is required, but no formal action.** These are responses to routine inquiries for information such as photographs, publications, comments, complaints or commendations which a standard form or general response is generated. These records lack substantive historical or evidential value and require no policy decisions or administrative actions. Retain the record for 3 years after cutoff and then destroy. DAA-0060-2014-0004-0002.

1. If after CRT sends a response, the writer sends additional correspondence without additional substantive information that changes the CRT response, send another form letter indicating that our prior determination remains and further correspondence will provide no useful purpose. Retain the record (an electronic copy of the incoming and CRT response) in the online portal for 3 years after cutoff and then destroy. DAA-0060-2014-0004-0002.
2. If the writer continues to write on the same matter (without providing any additional meaningful information), they are deemed a repeat writer under II.A.7. No response needed. Retain the original incoming letter for 1 year after cutoff and then destroy. DAA-0060-2014-0004-0001.

B. Monitor the situation, but no response immediately required. (General DJ Numbers are assigned to records that pertain to a variety of subjects and matters relating to a DJ Class but do not pertain to a specific case or investigative action involving DOJ/CRT.)
    1. For instance, 017 used by the Criminal Section is now called a General Number Temporary (GNT) file by DOJ. GNT files typically are correspondence or documents requiring few or no actions, and may contain correspondence or materials that have not developed into a case handled by DOJ/CRT. Retain for 10 years after cutoff and then destroy. N1-60-88-10/195C (until approval of DAA-0060-2017-0002).
    2. However, if a DOJ/CRT handled case or matter later develops out of the material, the section responsible for the records will open a formal DJ numbered case and move (or copy) the material from the GNT file into the DJ numbered case file. Once a good number is assigned, the material must be retained for the appropriate retention under the DJ Class.
C. No response issued, but materials maintained for documenting CRT's direction for litigating activities within the DJ Class (which DOJ now refers to as a General Number Permanent or GNP file). For instance, 012 used by the Voting Section are GNP files. These materials define or direct the overall litigation activities within the class. GNP files are permanent records, transferred to the National Archives and Records Administration (NARA) when 25 years old. N1-60-88-10/195C (pending approval of DAA-0060-2-17-0022-0001).

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

If an unauthorized user were to access the information collected by System, they would potentially access personally identifiable information for members of the public. Unauthorized users would potentially also access the narrative accounts shared by those who reported civil rights violations. Both would compromise the privacy of the reporting public. Such a breach could also compromise CRT's ability to carry out a future investigation effectively.

To mitigate against this possibility, the System will incorporate all required federal standards for information security for this level of information. [Staff is trained on how to properly handle

sensitive information. Non-disclosure agreements have also been executed to ensure proper use and protection of sensitive information. Access to the system is limited to a need to know. Rules of behavior and non-disclosure agreements for all users is required before access is provided. Access to the system is safeguarded by the use of PIV cards and/or RSA tokens. CRT staff also receives annual computer security awareness training regarding how to properly protect PII in accordance with Department of Justice standards.
Security controls commensurable to the National Institute of Standards and Technology-Federal Information Processing Standards Publications No. 199, "Standards for Security Categorization of Federal Information and Information Systems", are in place for CRT JCON. CRT adheres to the Department's Risk Management Framework (RMF) and creates a System Security Plan that will ensure CRT to follow strict DOJ NIST 800-53 Rev 4 core control standards]

Moreover, CRT intends to adhere to the records retention policy described above to purge records. In the short term, it will train any administrators overseeing the Portal on the appropriate records retention schedule, and charge them with executing it. In future versions, CRT will look to incorporate automatic purging consistent with the retention schedule.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X	
DOJ components	X			
Federal entities				
State, local, tribal gov't entities				
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or

agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Access to information gathered is restricted to be accessible only by those individuals who have been approved to work on the specific case or matter. Additionally, access to information gathered for
authenticating non-CRT individuals is restricted to be accessible only by the security staff. Further, all persons, including CRT personnel, accessing CRT data must sign the appropriate rules of behavior and non-disclosure agreement. CRT staff receives regular training in IT security and CRT
operations to understand what information is not appropriate for public release pursuant to the Freedom of Information Act.

Risk is mitigated by providing direct access on a need to know basis with restrictions on records and fields when necessary to reduce the need for bulk transfer of information. Access to data is provided to those who have a right to the data via their role in the process. Using the system with controls reduces mass exposure risk inherent in bulk transfers

In the event that CRT may need to share a particular report of a violation with another DOJ component for example, if CRT is coordinating with another DOJ component on litigation where a report of a violation is relevant – CRT does not intend to allow access directly. CRT personnel would duplicate and share a copy of the relevant report with known personnel of that DOJ component, with all applicable protections for PII.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: Individuals are not obligated to provide a report through the Portal. Moreover,

		most parts of the public-facing webform are optional for users. Finally, before submitting a report to CRT on the Portal, members of the public can review the report they would submit.
	No, individuals do not have the opportunity to decline to provide information.	Specify why not:

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: CRT has only one use for the information provided in the Portal to assist and advance its enforcement efforts by reviewing reports of potential violations from members of the public. Accordingly, if members of the public object to that use, they should not submit information to the Portal.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: 9/12/2019 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:

X	A security risk assessment has been conducted.	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: CSAM	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Splunk Enterprise collection of all logs,	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
	X	Training specific to the system for authorized users within the Department.
	X	Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

The security controls that protect the privacy of individuals and operations at CRT are set and maintained primarily by domain policy. Domain policy is a set of directions and controls that are stored on the primary authentication servers and are automatically applied to all computers and accounts within the domain. The controls force compliance to security policies to the extent possible.
The policies are automatically applied to all systems and accounts within the CRT operating unit upon logon or power up. The policies are maintained and validated by periodic scanning and system checks. The primary responsible technicians are the ISS system administrators and Service desk personnel.
All users accessing CRT data must sign the appropriate rules of behavior and non-disclosure agreement. Also, all CRT staff receives regular training in IT security and CRT operations
Access to databases is controlled on a case by case basis and can also be configured at a record by record or field by field basis on a need to know basis.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

	Yes, and the system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system:
X	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

See Section 1.

Impact Analysis

AMERICAN OVERSIGHT

Our hypothesis from the beginning of the engagement

We believe that

Providing **the public** with one common interface through which to submit complaints

providing the **Division** one interface from which to view and take action on complaints

Will….

Give people an easy and common interface to submit complaints

Provide the division with better routed & more complete complaints

Centralized source of truth for all incoming complaints (digital + physical)

Fosters transparency among the division

Increases the government's ability to provide remedies for civil rights violations and directing citizens

We know we have succeeded when:

SHORT TERM

Through end user testing...

1) Public users are able to complete the task and describe the process as user-friendly.

2) CRT users report that the system is reliable, fits their sections needs and is user-friendly.

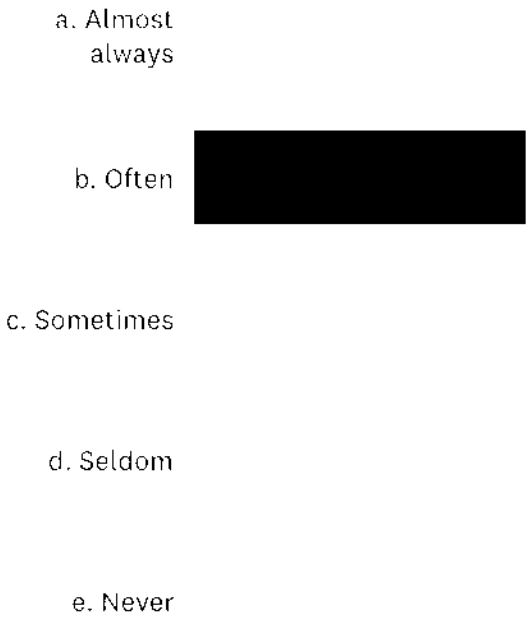
LONG TERM

When in production, we'd be able to track metrics like:

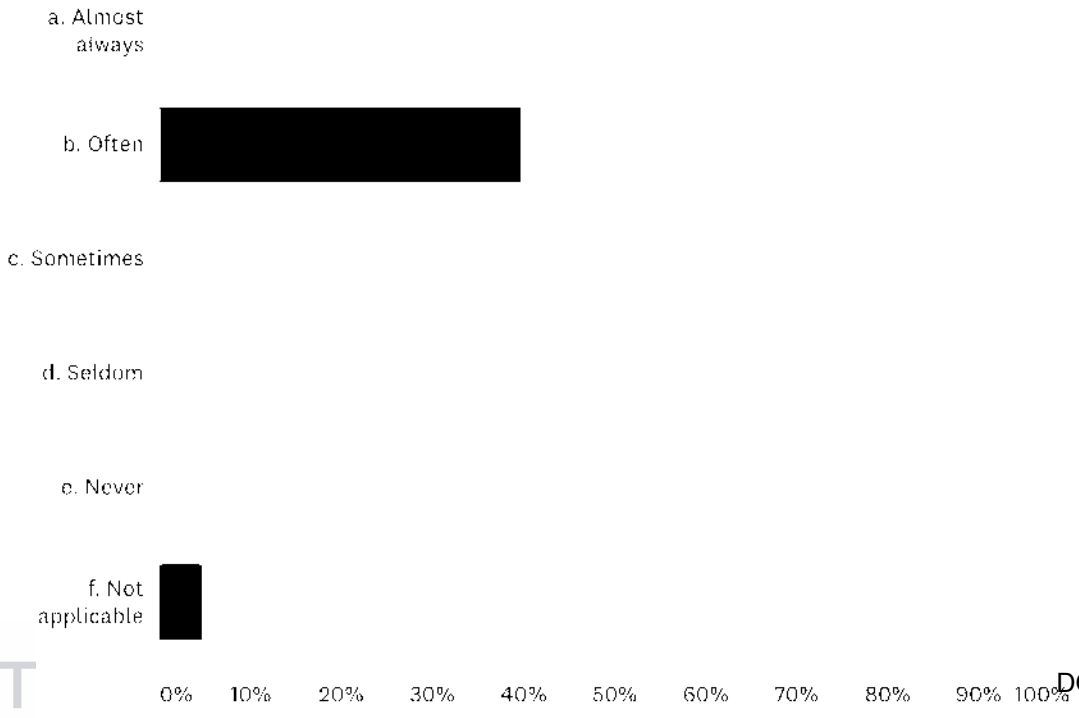
- **% of actionable complaints** ⬆
- **% of correctly routed complaints** ⬆
- **Response time to citizens** ⬇
- **Time spent processing complaints** ⬇

Better routed and more complete complaints

Actionable web reports via the portal



Section getting complaints they're in the best positioned to handle

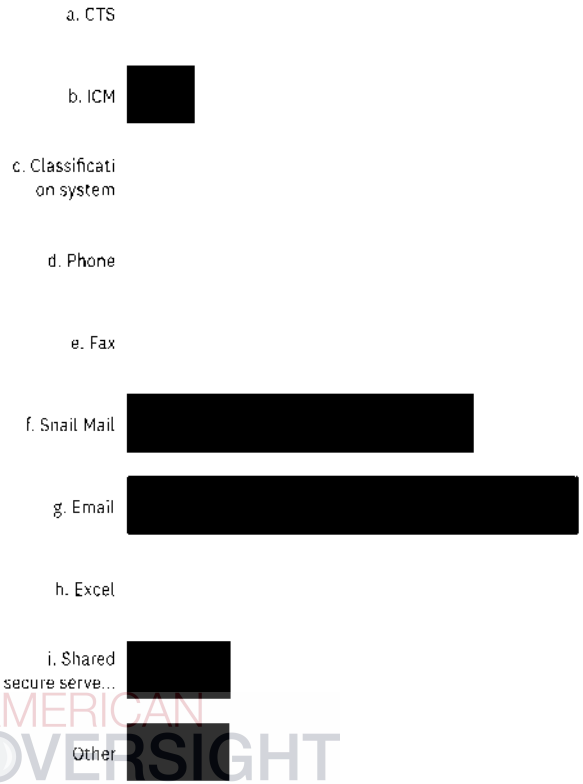


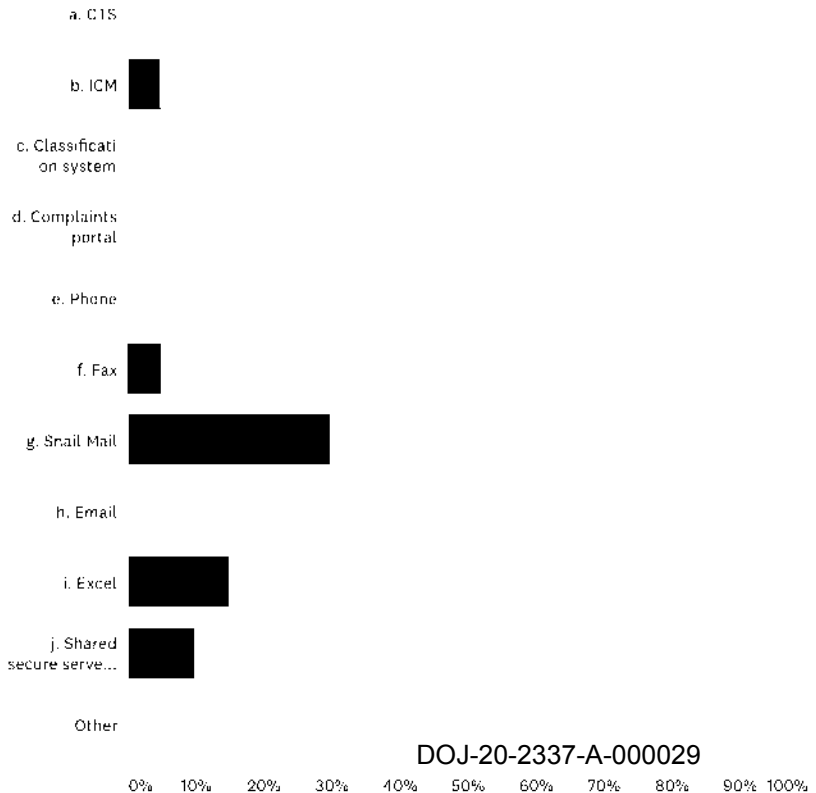
Improving efficiency

Time to process complaints (*before vs after*)

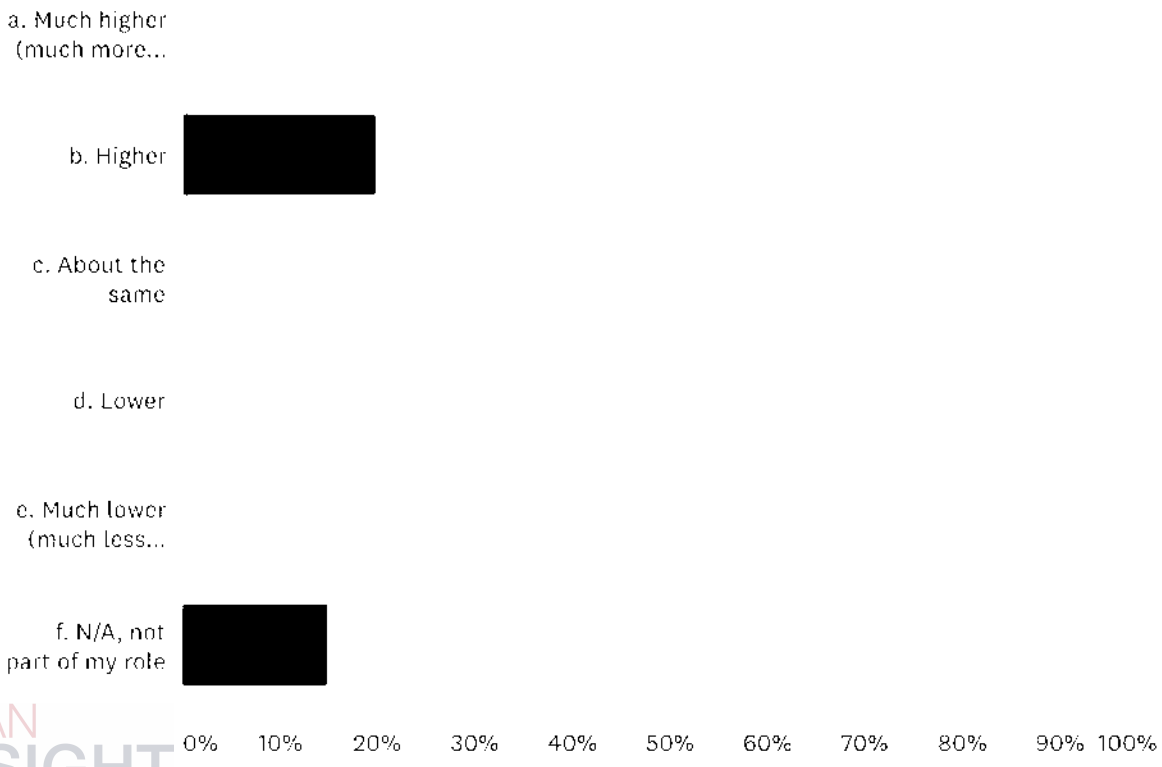
Number of systems used *(before vs after)*

Systems used *(before vs after)*

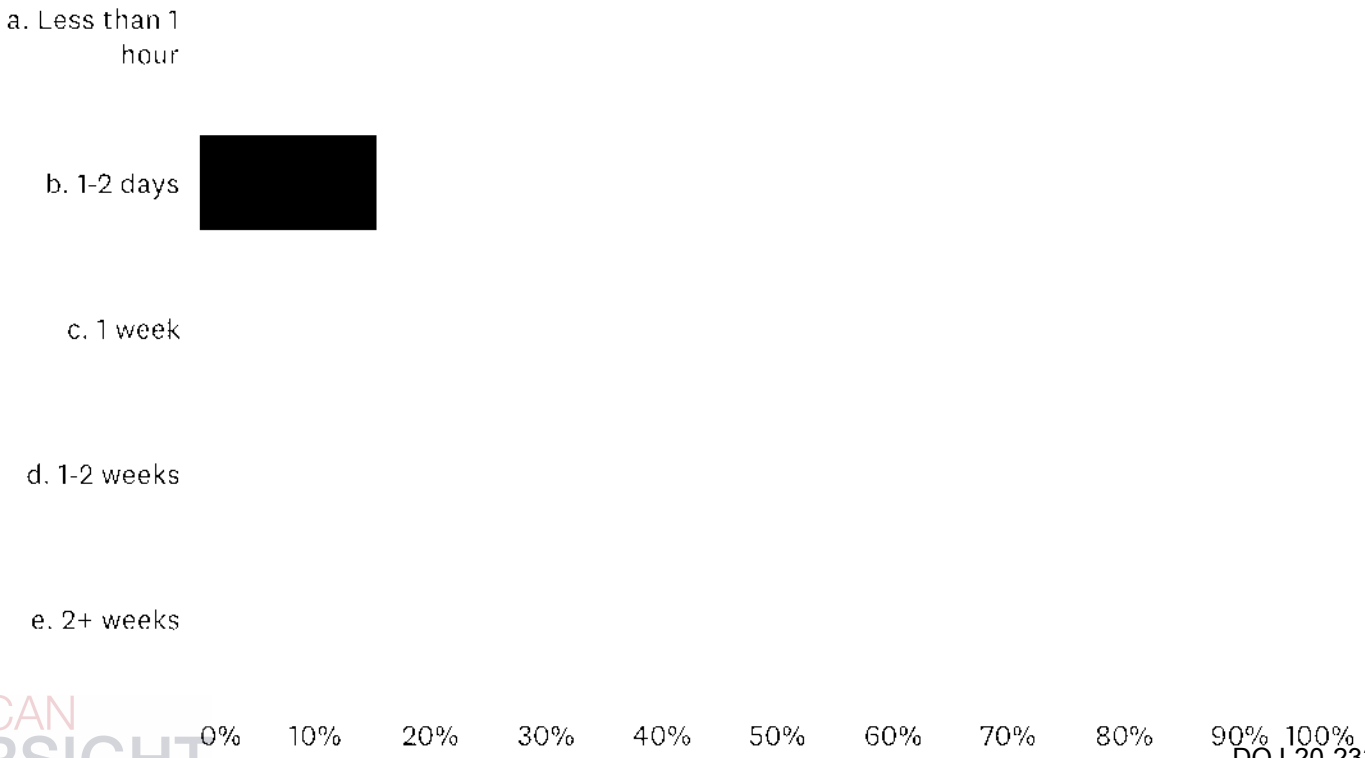




Manual work post Complaint Portal launch

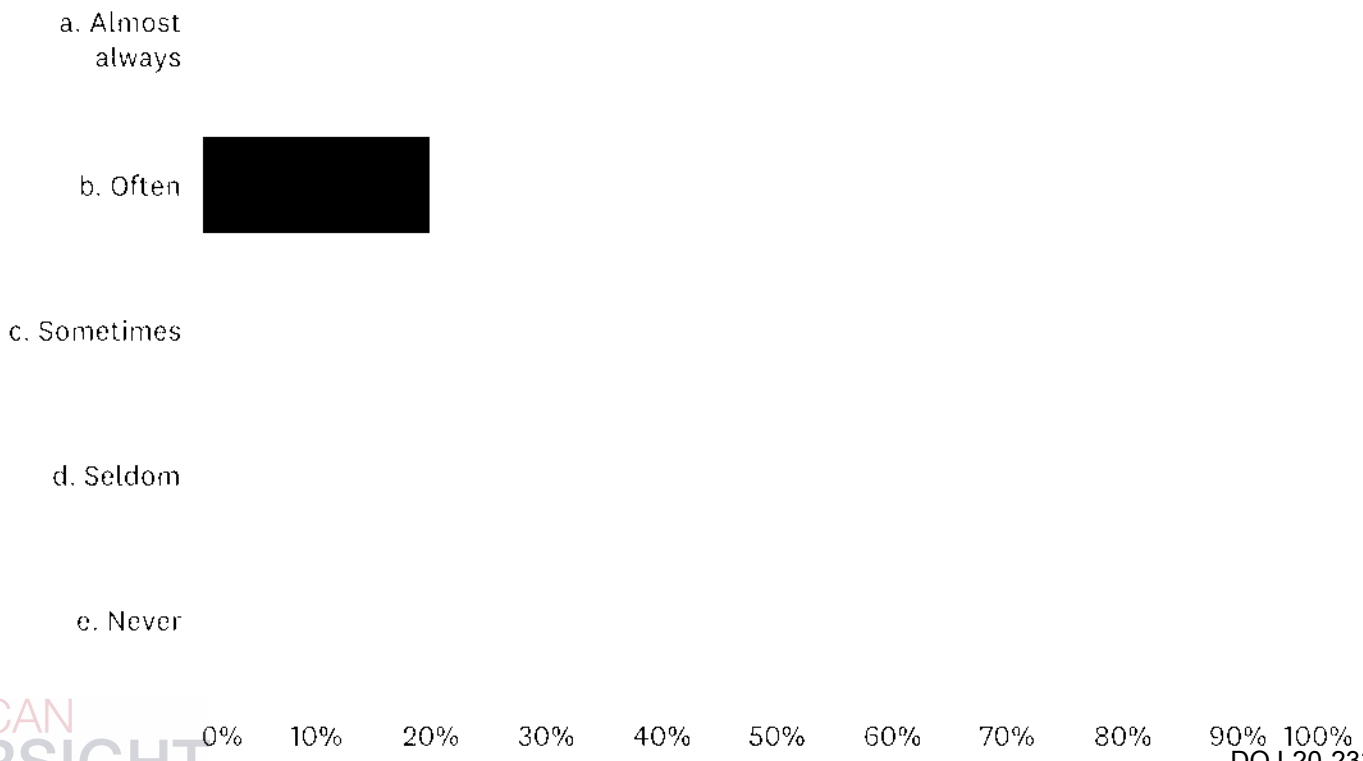


Time to process and resolve complaints

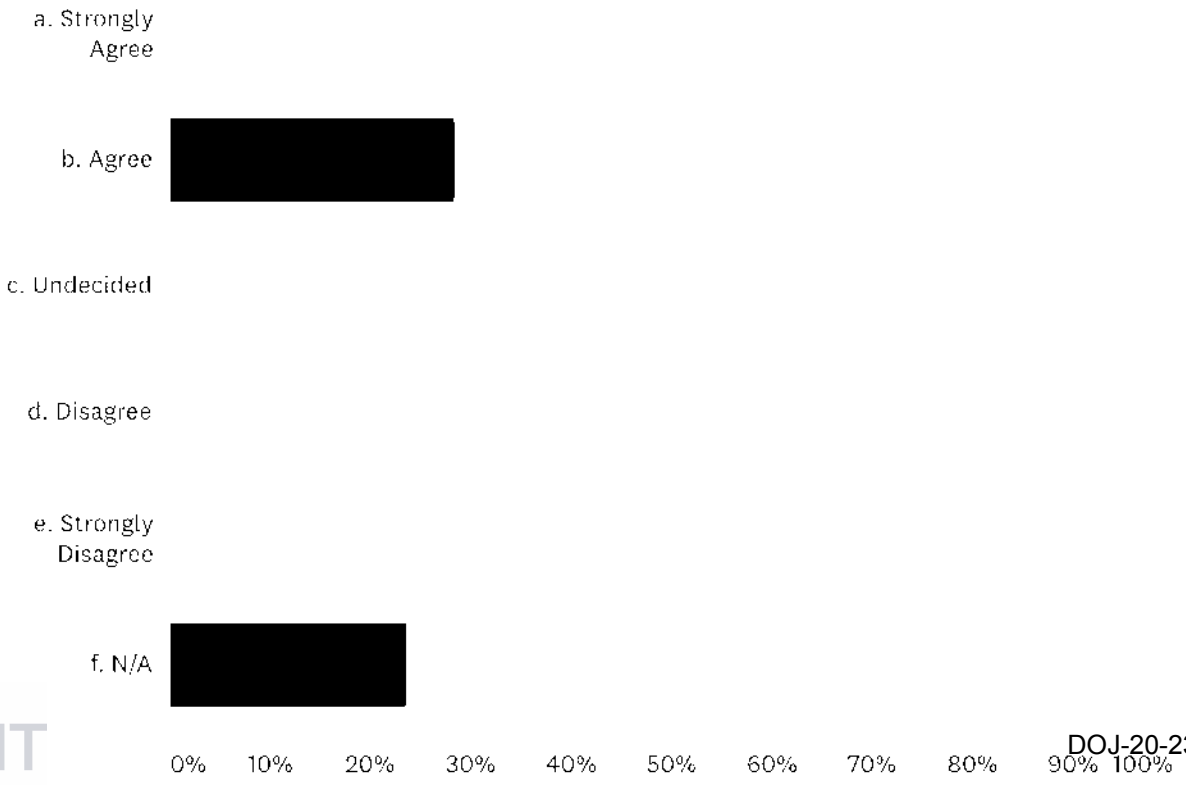


Centralized Source of truth and transparency

Referencing complaints to other sections

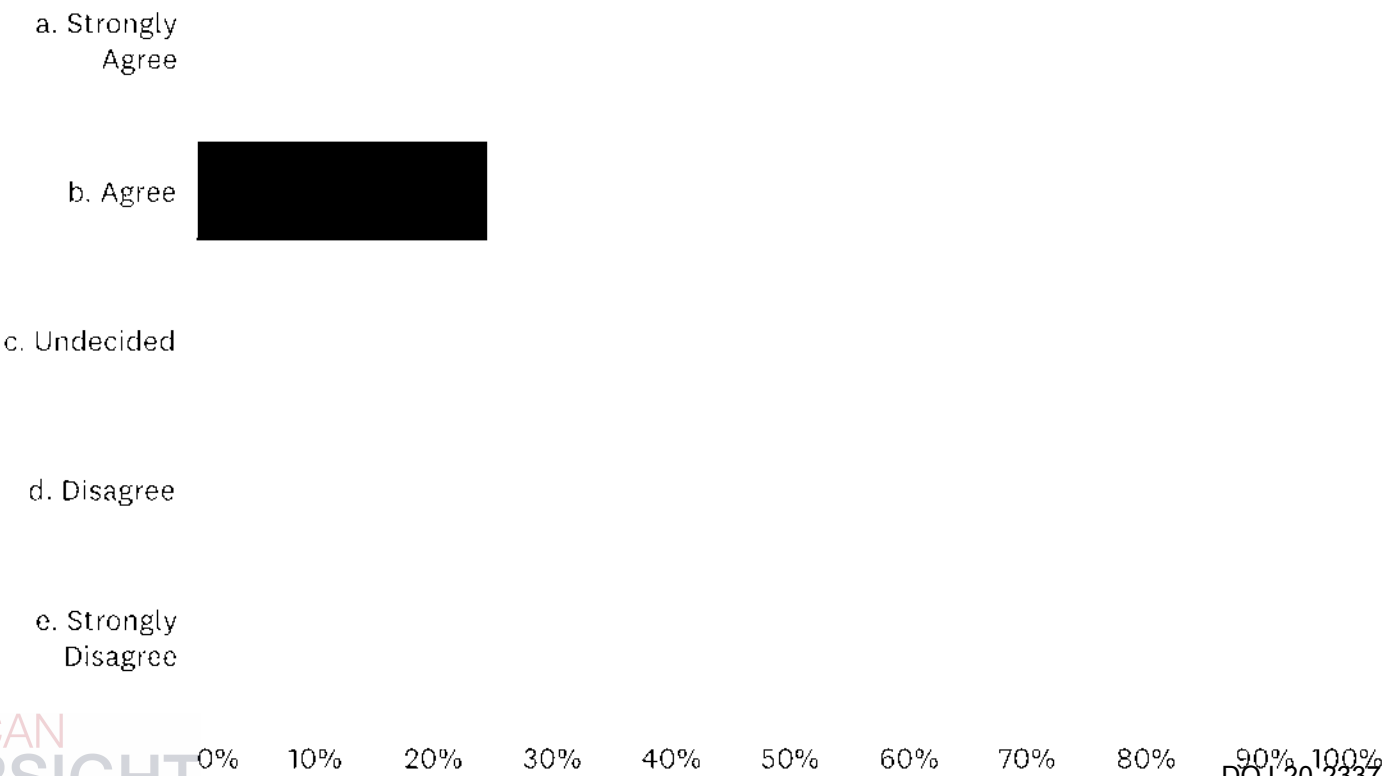


Helpful to collaborate with other sections



Mission Oriented work

Public has accurate expectations on how sections can help



Day-to-day section work supporting the mission