POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

City of Seattle Privacy Impact Assessment

NEXT GENERATION RECORDS MANAGEMENT FOR POLICE (NRMS) PROJECT

Owner: Seattle Police Department

12.7.2017

Seattle
Information Technology

CONTENTS

PURPOSE OF PIA

A Privacy Impact Assessment is designed to outline the anticipated privacy impacts from a City project/program or project/program update that collects, manages, retains or shares personal information from the public. The PIA will provide project/program details that will be used to determine how privacy impacts may be mitigated or reduced in accordance with the City of Seattle Privacy Principles and Privacy Statement.

ABSTRACT

Please provide a brief abstract. *The abstract is the single paragraph that will be used to describe the project and* ***will be published on the Privacy Program website.*** *It should be a minimum of three sentences and a maximum of four, and use the following format:*

- *The first sentence should include the name of the project, technology, pilot, or project/program (hereinafter referred to as "project/program").*
- *The second sentence should be a brief description of the project/program and its function.*
- *The third sentence should explain the reason the project/program is being created or updated and why the PIA is required. This sentence should include the reasons that caused the project/program to be identified as a "privacy sensitive system" in the Privacy Intake Form, such as the project/program requiring personal information, or the technology being considered privacy sensitive.*

The Seattle Police Department would like to conduct a privacy assessment on the "Next Generation Records Management for Police (NRMS)-CITP369" project (hereinafter referred to as NRMS). SPD is replacing its outdated records management system, Versadex, with modern technology and reformed business processes that include updating/adding integration points and migrating the existing data into a cloud solution known as Cobalt. This system is provided by Mark43 and focuses on readiness, training, and change management. It will be deployed in May 2019. The project solves numerous pain points as described in the business case. The PIA is required because NRMS will capture and retain personal information about crime victims, witnesses, other members of the public, including juveniles, and because NCIC/WACIC query returns information that is stored in the new solution containing personal 'people' information that is regulated by the FBI.

PROJECT/PROGRAM OVERVIEW

Please provide an overview of the project/program. *The overview provides the context and background necessary to understand the project/program's purpose and mission and the justification for operating a privacy sensitive project/program. Include the following:*

- *Describe the purpose of the system, technology, pilot or project/program; the name of the department that owns or is funding the project/program and how it the project/program relates to the department's mission;*
- *Describe how the project/program collects and uses personal information, including a typical transaction that details the life cycle from collection to disposal of the information;*

- *Describe any routine information sharing conducted by the project/program both within City of Seattle departments and with external partners. Describe how such external sharing is designed with the original collection of the information.*
- *Identify any major potential privacy risks identified and briefly discuss overall privacy impact of the project/program on individuals*
- *Identify the technology used and provide a brief description of how it collects information for the project/program.*

This project will solve the Seattle Police Department's record management concerns by replacing an outdated records management system with a system that promotes efficient business practices and transforms the department's technology processes. The police department has a duty to administer its limited the resources responsibly and effectively, while providing efficient and skillful police services. The NRMS accomplishes these goals by collecting accurate police reports, managing case investigations, evidence, and property, integrating with existing systems, and providing streamlined data extraction.

Seattle Police officers collect large volumes of personal and private information about individuals when they document, through a written report, the entire accounting of an incident. They document their written reports through the Department's record management systems (RMS). They collect detailed, personal information about people, including juveniles, victims of rape, and domestic violence victims. They collect information about people's property and their vehicles, including personally identifying information of crime victims and witnesses. The NRMS will retain this detailed demographic information about suspects, subjects, victims, and witnesses. It will retain social security numbers, information about mental health, medical care, drug and alcohol treatment, autopsy reports, information about vulnerable populations, and biometric data, such as fingerprints and DNA test results. As part of their investigations, officers may request information from NCIC/WACIC databases which are under regulatory control of the FBI though Washington State Patrol (WSP). NCIC/WACIC holds criminal information that Washington agencies enter about license plates, vehicles (stolen and otherwise wanted), wanted persons (warrants), missing persons, protection orders, person of interest, violent persons, unidentified persons, stolen guns, recovered guns, lost guns, stolen articles, recovered articles, stolen securities, stolen boats, and stolen vehicle parts. When an officer is responding to an incident, they conduct queries against state and federal databases (NCIC/WACIC) and receive returns of information from those databases, including prior arrests, prior addresses, other known names. This return of information is a 'point in time' and becomes part of the narrative of the officers' report and is therefore stored in the NRMS. These police reports are held indefinitely with no retention schedule for case management and investigations in the future.

SPD shares its police reports with the Seattle Law Department, the Seattle Municipal Courts, and the King County Prosecutor's Office using an open source technology known as the Enterprise Service Bus (ESB) also known as SeaJIS (Seattle Justice Information System). Less frequently, SPD may share this information manually with other law enforcement agencies for their investigations or warrant arrests. No other law enforcement agency has direct access to SPD's NRMS.

NRMS will capture and retain large volumes of personal and private information. The unauthorized disclosure of information from NRMS has the potential to cause significant harm. While SPD discloses a great deal of information to the public in response to public records requests and subpoenas, it applies the exemptions and privileges allowed under the Revised Code of Washington (RCW) to avoid violating an individual's privacy. In addition, SPD is audited on its use of NCIC/WACIC every three years to ensure its compliance with FBI's Criminal Justice Information Service (CJIS) security policies. Law enforcement

agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20, regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act).

The technology used includes the following components:

- Cloud based SaaS solution built on the "Amazon Web Services (AWS)" Government cloud platform
- Interfaces through the City of Seattle network perimeter with touch points to
  - Enterprise Service Bus (ESB) aka SeaJIS (Seattle Justice Information System)
  - Police Data Analytics Platform (DAP)

NOTIFICATION

1. ***How does the project/program provide notice about the information that is being collected?*** *Our Privacy Principles and Statement require that we provide notice to the public when we collect personal information, whenever possible.*
   - *Describe how notice will be provided to the individuals whose information is collected by this project/program and how it is adequate.*
   - *If notice is not provided, explain why not. (For certain law enforcement or other project/programs, notice may not be appropriate.)*
   - *Discuss how the notice provided corresponds to the purpose of the project/program and the stated uses of the information collected.*

   Arrested individuals are informed of their constitutional right to remain silent. This does not mean that they "opt out" of having information about them placed in the system. When the officer takes a police report, SPD policy specifies that they ask the victim, witness, and/or complainant whether they want a "do-not-disclose" attached to their information so that their identities will not be disclosed if the records are sought through a Public Records Act (PRA) request. SPD will still collect the information, but will limit disclosure of some of the information to the extent allowed by law. When SPD receives a request for information about an individual, SPD provides notice to the individual as provided in the PRA.

2. ***What opportunities are available for individuals to consent to the use of their information, decline to provide information, or opt out of the project/program?*** *Describe how an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use? If notice is provided explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. Note: An example of a reason to not provide an opt-out would be that the data is encrypted and therefore unlikely available to identify an individual in the event of a data breach.*

   Given the nature of law enforcement records, individuals do not have the right to condition the use of information gathered; however, when the officer takes a police report, SPD policy specifies that officers ask the victim, witness, and/or complainant whether they want nondisclosure of their identities for purposes of the PRA.

COLLECTION

3. ***Identify the information, including personal information, that the project/program collects, uses, disseminates, or maintains.*** *Explain how the data collection ties with the purpose of the underlying mission of the department.*

   The NRMS collects information similar to the previous RMS. Police report information includes information about events such as:

   - Police action event information including:
     - Date, time, reporting officer, agencies on scene, reporting party
   - Offence(s) information including:
     - Bias or hate motivations, offence location, officer narratives, victim information, suspect information, witness information
   - Gang involvement
   - Family and domestic violence
   - Personal information including
     - Name, sex, race, ethnicity, social security number, date of birth, driver's license number, phone number(s), employer, linkage factors, relationships, age or age range, height, weight, complexion, build, hair color, hair style, facial hair style, clothing details, identifying marks, scars and tattoos, aliases, FBI ID number
   - Property information
     - Status, description, serial number, quantity, current location, make, color, evidence tag number, value loss, chain of custody information
   - Vehicle information
     - Make, model, VIN, license plate, vehicle category, description, year, color, registration information, mileage, insurance information, associated person, status, value, impound information

   The data collection ties to the law enforcement mission of the department.

4. ***Is information being collected from sources other than an individual, including other IT systems, systems of records, commercial data aggregators, publicly available data and/or other departments?*** *State the source(s) and explain why information from sources other than the individual is required.*

   The NRMS is the technologically-advanced equivalent of paper police investigation files. Information in the system will be collected from multiple sources. In addition to the NCIC/WACIC information discussed above, it will contain information from SPD's Computer-Aided Dispatch (CAD), COBAN In-Car Video System, Evidence.Com Body-worn Video System, the NICE 911 logging recorder system, and approved reports from the Coplogic online SaaS solution where Seattle community members enter nonemergency police reports. Due to the nature of law enforcement investigations, information from other SPD systems, as well as information from outside sources, and publicly-available data may be entered in the system.

USE

5. ***Describe how and why the project/program uses the information that is collected****. List each use (internal and external to the department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used.*

The information being collected will be used for a variety of purposes including, but not limited to:

1. Supervisory review
    a. Supervisors may review reports entered to determine if departmental policies were being followed by an officer in the course of their duties.
2. Reviewing reports in the course of a use-of force complaint/investigation
    a. Reports may be used by internal investigations centered on whether inappropriate uses of force were used in the course of an officer's interaction with the public.
3. Training purposes
    a. In order to improve the training of officers, reports illustrating appropriate and/or inappropriate interaction with the public may be used as a training tool.
4. Criminal investigations
    a. The NRMS will document the investigation from inception until it is referred to the prosecuting authority to be used in prosecution.
5. Public disclosure
    a. The public may request reports and data in NRMS from the department in accordance with the public disclosure laws of Washington State.
6. Criminal prosecution
    a. Prosecutors will review their reports to assist them in determining if an incident is to be prosecuted by the City or County.
7. Evidence in a prosecution filed in a court of law
    a. If a case is filed in a court of law, the prosecutor, defense, and the court will use the report in the course of the case.

6. ***Does the project/program use technology to:***

a. ***Conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly or***

b. ***Create new information such as a score, analysis, or report?***

If so, state how the City of Seattle plans to use such results. Some project/programs perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Explain what will be done with the newly derived information. Will the results be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data?

The NRMS will provide a more robust ability to search and query data in the system. This provides a significant advantage to SPD for immediate access to information for investigative, accountability and training purposes, as described in the response to Question #5, above. The information could be queried or analyzed to enhance SPD's ability for example to deploy its officers or to identify concerns about officer behavior that warrants intervention.

SPD will use data from the NRMS to create new reports, such as investigative incident reports, reports illustrating compliance with the Department of Justice (DOJ) consent decree, reports regarding different categories of crime, etc. It will be used to analyze the type of crimes that are occurring, where they are occurring, trends over time, and the effectiveness of efforts to respond to those categories of crime. The NRMS will enhance SPD's ability to perform these current functions.

7. ***How does the project/program ensure appropriate use of the information that is collected?*** *Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.*

   Supervisors and commanding officers are responsible for ensuring compliance with policies.
   All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.
   All authorized users of NRMS must be CJIS certified and must maintain Washington State ACCESS certification. SPD Policy 12.050 defines the proper use of criminal justice information systems.

RETENTION

8. ***Does the project/program follow the City records retention standard for the information it collects?*** *Departments are responsible for ensuring information collected is only retained for the period required by law. City departments are further responsible for reviewing and auditing their compliance with this process. For more information, please see the internal retention schedule, here, and records retention ordinance, here.*

   In addition, please provide answers to the following questions:
   - *How does it dispose of the information stored at the appropriate interval?*
   - *What is your audit process for ensuring the timely and appropriate disposal of information?*

   SPD retains the information stored in its RMS indefinitely, and no disposal of information occurs.

SHARING

9. ***Are there other departments or agencies with assigned roles and responsibilities regarding the information that is collected?*** *Identify and list the name(s) of any departments or agencies with which the information is shared and how ownership and management of the data will be handled.*

Multiple agencies will be handling the data as part of the discovery process around criminal cases:

- City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private criminal defense attorneys
- Seattle Municipal Court

- King County Superior Court

The data will also be shared with Washington State Patrol and other law enforcement agencies conducting investigations.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20, regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act).

10. *Does the project/program place limitations on data sharing?*

Describe any limitations that may be placed on external agencies further sharing the information provided by the City of Seattle. In some instances, the external agency may have a duty to share the information, for example through the information sharing environment.

No person, outside of SPD and Seattle IT, has direct access to NRMS. Prosecutorial and law enforcement agencies will have access to information in the NRMS for the purposes of prosecution of crimes. Individual pieces of information may be shared with other law enforcement agencies in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20, regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act).

Typically, this information and evidence is not disclosable to the public while it is part of an on-going investigation. Once it moves to the court system, it becomes part of the public record.

Any State agency that acquires the data is subject to PRA, and Federal agencies are subject to the Federal Freedom of Information Act (FOIA). As a result, these agencies are obligated to disclose records to the public upon request. Similar to SPD, they would apply applicable exemptions to redact or withhold exempt information prior to disclosure.

11. *What procedures are in place to determine which users may access the information and how does the project/program determine who has access?* *Describe the process and authorization by which an individual receives access to the information held by the project/program, both electronic and paper based records. Identify users from other departments who may have access to the project/program information and under what roles these individuals have such access. Describe the different roles in general terms that have been created that permit access to such project/program information. Specifically, if remote access to the system is allowed or external storage or communication devices*

interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication).

Access to NRMS is based on the role and unit assignment within the SPD organization. Roles vary based on the needs of the assignment and include view only access, report writing, report approval, evidence access, investigation access, and data center approval. This solution is configured similar to the previous solution. Assigned Seattle IT users may have some level of access to NRMS for systems support.

Two-factor authentication is required to access NRMS.

12. ***How does the project/program review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?*** *Please describe the process for reviewing and updating data sharing agreements.*

    Prior to sharing data from the NRMS, SPD will produce properly executed research and confidentiality agreements as provided by SPD Policy 12.055 with the sharing agencies.

LEGAL OBLIGATIONS AND COMPLIANCE

13. ***Are there any specific legal authorities and/or agreements that permit and define the collection of information by the project/program in question?***
    - *List all statutory and regulatory authority that pertains to or governs the information collected by the project/program, including the authority to collect the information listed in question.*
    - *If you are relying on another department and/or agency to manage the legal or compliance authority of the information that is collected, please list those departments and authorities.*

    - WA State Patrol (WSP) is the regulatory authority for the NCIC/WACIC information only.
    - King County (no known audits other than WSP)
    - Seattle Municipal Courts (no known audits other than WSP)
    - Seattle Law (no known audits other than WSP through Police department)
    - Mark43 is the vendor and will undergo CJIS Security Compliance audits conducted jointly by the Police department as the procuring agency and the WA State Patrol (WSP).
    - Seattle Municipal Code and SPD Manual policies regarding the collection of information also apply.

14. ***How is data accuracy ensured?*** *Explain how the project/program checks the accuracy of the information. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. If the project/program does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project/program.*

    Officers are required to enter accurate information into the system. Reports are reviewed and approved by supervisors in the report writer's chain of command. The project includes scope for business process engineering that will ensure frequent quality control procedures for data accuracy.

15. ***What are the procedures that allow individuals to access their information?***
Describe any procedures or regulations the department has in place that allow access to information collected by the system or project/program and/or to an accounting of disclosures of that information.

SPD is subject to the PRA and must disclose records to anyone who requests them. SPD will apply applicable exemptions to redact or withhold exempt information prior to disclosure. Once disclosed, SPD has no control over how the requestor uses the information.

The information may also be disclosed pursuant to subpoena. SPD would redact information as permitted before disclosure. Once disclosed pursuant to a subpoena, the data may be subject to applicable court rules, or in some cases, a protective order. The court rules would apply to any data submitted to a court in connection with a criminal or civil case.

SPD maintains a log of all PRA requests and a log of all subpoena responses.

The data may also be disclosed to researchers pursuant to a Research Agreement. SPD ensures that all Research Agreements include non-disclosure, storage, and use restrictions necessary to protect the data.

16. ***What procedures, if any, are in place to allow an individual to correct inaccurate or erroneous information?*** *Discuss the procedures for individuals to address possibly inaccurate or erroneous information. If none exist, please state why.*

When officers collect information that is inaccurate, it is usually retained as part of the accounting of the incident. Once a police report is approved, and an officer learns of inaccurate information in the report, they may file supplemental reports that include the corrected information. Any information in NRMS that is appended or changed is logged in auditable records.

17. ***Is the system compliant with all appropriate City of Seattle and other appropriate regulations and requirements?*** *Please provide details about reviews and other means of ensuring systems and project/program compliance.*

Per SPD Policy 12.111, "The Seattle Police Department receives information from the FBI's Criminal Justice Information Service (CJIS) and must comply with the CJIS security policy and the rules governing the access, use, and dissemination of CJIS information found in Title 28, Part 20, CFR." NRMS has undergone Privacy, Security, Risk, Compliance, and Service Acceptance Criteria reviews by Seattle IT. The NRMS project uses the standard Financial Workbook used across all Project Management Office projects. .

18. ***Has a system security plan been completed for the information system(s) supporting the project/program?*** *Please provide details about how the information and system are secured against unauthorized access.*

NRMS authorization is role-based and limited to ACCESS certified SPD employees and requires two-factor authentication. In addition, an industry standard SOC2 security audit has been conducted at implementation with additional SOC2 audits to be completed along with intrusion testing annually.

19. ***How is the project/program mitigating privacy risk? G****iven the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.*

    The nature of the Department's mission will inevitably lead the collection and maintenance of information that many may believe to be private and potentially embarrassing. Minimizing privacy risks revolve around disclosure of personally identifiable information.

    All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.
    Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

    The project has implemented role-based access to NRMS with two-factor authentication as an additional layer to mitigate the risk of unintended release of privacy information.

MONITORING AND ENFORCEMENT

20. ***Describe how the project/program maintains a record of any disclosures outside of the department.*** *A project/program may keep a paper or electronic record of the date, nature, and purpose of each disclosure, and name and address of the individual or agency to whom the disclosure is made. If the project/program keeps a record, list what information is retained as part of the accounting requirement. A separate system does not need to be created to meet the accounting requirement, but the project/program must be able to recreate the information noted above to demonstrate compliance. If the project/program does not, explain why not.*

    The Public Disclosure Unit (PDU) manages Public Disclosure Requests (PDR) and has an excellent auditing ability. PDU employees the GovQA PDR processing application. It meets the required security and privacy standards. It provides a detailed history of every PDR processed and log reflecting ever PDR disclosure. NRMS also maintains comprehensive and auditable release tracking within the system itself.

    SPD also tracks all subpoena disclosures.

21. ***Have access controls been implemented and are audit logs are regularly reviewed to ensure appropriate sharing outside of the department?*** *Is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies? Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

    Outside agencies do not have direct access to NRMS.

22. ***How does the project/program ensure that the information is used in accordance with stated practices of the project/program?*** *What auditing measures are in place to safeguard the information*

and policies that pertain to them? Explain whether the project/program conducts self-audits, third party audits or reviews.?

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. Any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

Annually, the SPD solution owners will conduct a review of the SOC 2 Type 2 audit report provided by the Mark43 vendor. The SOC 2 audit report is an industry standard technical and procedure audit developed by the American Institute of CPAs for service providers who store customer data in the cloud. Other audits, including a quarterly user roles audit, will be identified during the implementation activity of the project.

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any system at any time. The Office of Inspector General and the federal monitor can also audit for compliance at any time.

23. ***Describe what privacy training is provided to users either generally or specifically relevant to the project/program.*** *City of Seattle offers privacy and security training. Each project/program may offer training specific to the project/program, which touches on information handling procedures and sensitivity of information. Discuss how individuals who have access to personal information are trained to handle it appropriately. Explain what controls are in place to ensure that users of the system have completed training relevant to the project/program.*

All authorized users of NRMS must be CJIS certified and must maintain Washington State ACCESS certification. SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. Any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

Is there any aspect of the project/program that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information? *Examples might include a push of information out to individuals that is unexpected and appears to be intrusive, or an engagement with a third party to use information derived from the data collected that is not explained in the initial notification.*

It is possible that the public may be concerned if information from NRMS is part of a prosecution or released to the public thorough media or the internet. Those concerns cannot be mitigated by the City or SPD without significant changes to state criminal and/or public disclosure laws.

At the same time, the NRMS will enhance privacy within the strictures of the PRA because the NRMS provides a significantly improved ability to locate and redact exempt information, to identify and flag records that are subject to court sealing, and to process PDRs in general.