The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).


Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.
Privacy Impact Assessment for the VA IT System called:

Assessing Social and Community Environments with National Data (ASCEND) for Veteran Suicide Prevention: Development Phase

VA Eastern Colorado Health Care System (ECHCS) Mental Illness Research, Education and Clinical Center (MIRECC) for Suicide Prevention

Date PIA submitted for review:

11.03.2020

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts Table</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Christian Loftus</td>
<td><a href="mailto:Christian.loftus@va.gov">Christian.loftus@va.gov</a></td>
<td>(859) 281 - 2470</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Mark McGee</td>
<td><a href="mailto:James.mcggee5@va.gov">James.mcggee5@va.gov</a></td>
<td>520-629-4834</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Tristan Carroll</td>
<td><a href="mailto:Tristan.carroll@va.gov">Tristan.carroll@va.gov</a></td>
<td>210-993-2068</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Melanie Reed</td>
<td><a href="mailto:Melanie.reed2@va.gov">Melanie.reed2@va.gov</a></td>
<td>720-723-8610 or 907-378-1697</td>
</tr>
</tbody>
</table>
Abstract

The abstract provides the simplest explanation for “what does the system do?” and will be published online to accompany the PIA link.

Assessing Social and Community Environment with National Data (ASCEND) for Veteran Suicide Prevention is a VA Office of Mental Health and Suicide Prevention (OMHSP)-funded operations project aiming to enhance surveillance of non-fatal suicidal self-directed violence (NF-SSDV) among Veterans. It is widely recognized that routine, national surveys can serve as valuable surveillance tools for tracking health-related behaviors. Thus, one of the most promising approaches to documenting the prevalence of NF-SSDV among Veterans and tracking changes in these estimates over time is to use data from reoccurring, nationally representative surveys. As such, the overarching goal of this project is to design and implement a reoccurring national survey of Veterans (ASCEND) that will:

1. Serve as a national surveillance system to document prevalence and trends over time in non-fatal suicidal self-directed violence (NF-SSDV; i.e., suicide ideation [SI] and suicide attempt [SA]) across the life course (e.g., lifetime, post-military service, past-year); and

2. Provide estimates of the impact of social and community risk and protective factors (e.g., social determinants of health, social capital, and interpersonal needs) on SI and SA among Veterans.

This project will focus on the Veteran population as a whole, not only those using VHA services, and will inform policy and service development, program evaluation, and quality improvement for Veteran suicide prevention.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
• Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
• A citation of the legal authority to operate the IT system.
• Whether the completion of this PIA will result in circumstances that require changes to business processes.
• Whether the completion of this PIA could potentially result in technology changes.
• If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
• Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.
• Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
• NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?
• What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?

In collaboration with the Department of Veteran Affairs and the ECHCS Mental Illness Research Education and Clinical Center (MIRECC) for Veteran Suicide Prevention (VA), Minuteman Technology Services (MTS) and NORC at the University of Chicago (NORC) are working to develop a national survey, ASCEND for Veteran Suicide Prevention, to enhance surveillance of non-fatal suicidal self-directed violence (NF-SSDV) among Veterans. Through reoccurring administration (i.e., annually with different samples), the long-term goal of ASCEND is to track the prevalence and trends over time in NF-SSDV within the broader veteran population, as well as risk of NF-SSDV among veterans over time in relation to community and individual-level risk and protective factors. Results will be used to inform policy and service development, program evaluation, and quality improvement for veteran suicide prevention. This first iteration of ASCEND aims to collect responses from a nationally representative group of 50,000 Veterans.

The VA Eastern Colorado Health Care System (ECHCS) MIRECC has awarded contract #36C25919Q0310 to MTS to perform ASCEND-related study tasks for the period of performance of one year, with two option years, from the contract start date of June 1, 2019. The ECHCH and MTS also have a business associate agreement (BAA) in place. MTS, as the prime contractor, has subcontracted with NORC to perform data collection. Both MTS and NORC will have access to ASCEND system data for the purposes of completing study tasks. In addition, data will be shared with Acxiom and PressAmerica for the study tasks described below.

Specific deliverables/tasks that describe the data transfer collection requirement are below:

---

1 NORC is not an acronym, it is the company's name, as with organizations such as IBM, AT&T, RAND, and GEICO.
4.2.4 The contractor shall need to document an existing or obtain in new a VA Authority To Operate (ATO). This shall be necessary to have in place prior to the start of contract option year one, in order to collect geographic location data and other Personally Identifiable Information (PII) (e.g., name, SSN) from survey participants. Given the time required to obtain a new ATO, the contractor shall have all necessary security requirements in place to obtain an ATO at the time of contract initiation.

4.2.5 The contractor shall develop the multi-stage sampling design and frame for ASCEND using the USVets database for both the pilot and the initial wave of data collection. The survey shall focus on the Veteran population as a whole, not only those using VHA services. The total sample size for this survey is expected to be approximately 50,000 Veterans. The final sample size and sampling approach shall be developed within the scope of this contract, in partnership with VA PIs and the engagement boards. The contractor shall be responsible for completing:

- Power analysis to finalize survey sample size
- Development of the multi-stage sampling design
- Sampling frame
- Updates to Veteran contact information prior to recruitment (using, for example, Lexis Nexis, National Change of Address, Credit Bureau, or other comparable databases). The contractor shall report to the COR all Veterans with incorrect address information and the extent to which they have succeeded in locating the correct address. The contractor shall compute error rates for addresses by source of address information (Department of Defense, Internal Revenue Service, and VA). The contractor shall create an electronic database consisting of the name, each address and any other available contact information for each member of the target survey sample. Each address provided to the contractor shall be included, together with a variable denoting whether the final recruitment address was “good” or “not delivered.”

In order to survey a nationally representative sample of US Veterans, including those who use VHA services as well as those who do not, ASCEND will use the United States Veterans Eligibility Trends and Statistics (USVETS) database and the VA Department of Defense Identity Repository (VADIR) as sampling frames. Once drawn, the sample data set will be transferred via SFTP or via mail from the MIRECC’s research data drive to NORCs computing environment for data collection and recruitment. NORC will use Acxiom to update phone numbers, mailing and email addresses for the sampled Veterans. PressAmerica will receive, through secure file transfer, the names, full addresses, study IDs, and PIN numbers for the Veterans in the selected sample and will mail a series of recruitment materials. NORC will use Voxco, a data collection and survey administration platform which is installed on NORC’s physical servers, to administer the study survey. This instance of Voxco (and the entirety of the ASCEND system) does not use cloud technology and Voxco (the company) will not receive any ASCEND data. Potential respondents will be able to respond to the survey over the phone, or online via the mobile, tablet, or desktop internet browser (no application download required). Following the conclusion of ASCEND data collection, the survey response data will remain in the vendor’s (i.e.,

---

2 PIN numbers are unique, randomly generated combinations of characters and numbers that are in no way related to the Veteran’s PII. NORC sampling specialists will assign PIN numbers to the selected sample once it has been drawn. Veterans will use PIN numbers to access the web-based survey instrument.
NORC) computing environment for the tasks of data analysis, data merge with community-level data
sources, and results reporting. All electronic data will be stored behind NORC’s firewall. As requested,
and required by the contract #36C25919Q0310, NORC shall submit interim data sets back to the VA
following both periods of data collection. Transfer of the data set shall be accomplished by a VA-
approved SFTP or by the alternative mailing option.

Data disseminated for use in this contract (to include PII and other controlled unclassified information
CUI) will reside at more than one site. The VA ISSO team shall maintain security oversight of all data,
and system reciprocity will not be observed during mean time periods between VA assessments.
Security controls shall remain consistent across sites, and continuous monitoring processes shall be
imparted at contractor sites. Any anomaly detected shall be investigated and security incidents will be
reported to VA Security Officers immediately. Architectural elements have been submitted and will
address security relevant build specks, such that the result of this PIA should not impact either business
processes, or technical changes.

The legal authority to operate this project falls under Title 38, United States Code, chapter 73, section
7301. The information collected is contained within the System of Records for VADIR— VA
SOR#138VA005Q, as well as within USVETS, which falls under three active SORs: Health Program
Evaluation - SOR# 107VA008B; Non-Health Data Analyses and Projections for VA Policy and
Planning—SOR# 149VA008A; Veterans, Service Members, Family Members, and VA Beneficiary
Survey Records- SOR# 43VA008.

This system does not use cloud technology.
Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy-Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Other Unique Identifying Number as needed for identifying duplicates between sampling frames

In addition to the above, the ASCEND project will collect the following information from VA databases (ie: United States Veterans Eligibility Trends and Statistics (USVets) and the VA/DoD Identity Repository (VADIR)) for the purposes of identifying the recruitment sample and completing other key study tasks:

- Indicator for whether person was living at the end of FY 2017 (or most recent FY available)
- Gender
- Transition status
- Maximum separation date
- Veteran status
- VHA usage information
• Years of service
• Retirement indicator
• Branch
• Rank
• Wars served in
• Character of service
• Components served in
• Branch of most recent separation
• Benefits used

In addition, the ASCEND survey will survey responses related to the following domains of study for Veterans who choose to participate in and complete the survey:

• Military history
• Health status (PROMIS Global Health)
• Depression status (PHQ-9)
• Lifetime history of self-directed violence
• Exposure to suicide
• Perceptions about suicide
• PTSD (PC-PTSD-5)
• Alcohol and drug use (Addiction Severity Index/CAGE)
• Trauma history (ACES)
• Access to lethal means
• Healthcare utilization (GHSQ, HSRQ, BTM, NSV)
• Social support (NIH Toolbox)
• Social functioning and satisfaction (Well-Being Inventory)
• History of intimate partner violence (E-HITS)
• Neighborhood/Community environment (Sampson & Raudenbush, Inclusion of Self in Community Scale)
• Community problems (WHO)
• Involvement in virtual or online communities
• Barriers to treatment (BACE-3)
• Demographics: age, sex assigned at birth, gender, race and ethnicity, education level, marital status, sexual orientation, employment status, income level, household size, homeless status, history of felonies and/misdemeanors

PII Mapping of Components

ASCEND consists of 3 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by ASCEND and the reasons for the collection of the PII are in the table below.
## PII Mapped to Components

### Components Table

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting PII</th>
<th>Does this function collect or store PII? (Yes/No)</th>
<th>Type of PII</th>
<th>Reason for Collection of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORC SQL Database</td>
<td>Yes</td>
<td>Full name, study ID and PIN, address, email address, DOB, gender, ethnicity, race, transition status</td>
<td>Telephone interviewers will use the PII in the database to contact potential respondents for the purpose of completing the survey over the phone. The Voxco data collection software uses the PII to intelligently suggest the best phone to call next, based on key demographics, so that a representative sample of responses can be collected.</td>
<td>All PII, and data otherwise CUI, shall be governed in accordance with the NIST security framework, FedRAMP:Moderate” technical controls, and FIPS approved encryption levels. SQL database security is described in more detail in Appendix B.</td>
</tr>
<tr>
<td>NORC SFTP File Server</td>
<td>Yes</td>
<td>Full name, SSN, study ID and PIN, full address, telephone number, email address, DOB, gender, ethnicity, race, transition status</td>
<td>Receives and transfers sample data and response data to and from the VA.</td>
<td>Data shall be transited from NORC’s system to VA, via FIPS approved SFTP or via mail. All data (bi-directional) to be transferred via Secure File Transfer Protocol (SFTP) will use port 22, and using FIPS</td>
</tr>
<tr>
<td>Data Source</td>
<td>PII Used</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VA MIRECC Research Data Drive</td>
<td>Yes</td>
<td>Full name, SSN, Full address, Telephone number, Email address, Date of birth, Gender, Ethnicity, Race&lt;br&gt;The requested data sets from USVETs and VADIR will be stored on the VA MIRECC Research Data Drive. PII will be used to draw a nationally representative sample of Veterans. The sample data set will be transferred. All PII on the VA MIRECC Research Data drive will be stored behind the VA firewall and will be user-restricted and/or password protected such that only appropriate members of the study team will have access.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Data will be approved, 256-bit encryption, and shall be encrypted prior to transfer, hash validated and remain in encrypted at rest (upon arrival). Data will be stored in a secure SQL Database, that shall be detailed within Architectural documents. All system hardening shall be done in compliance with FedRAMP Moderate controls. Data shall not be used for any purpose other than intended and will be shared in accordance with contracts and business agreements.
1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

There are 4 sources of information for the ASCEND system.

Two data sets are being used to develop the sampling frame for the ASCEND study:

1. USVETS is a national database of Veterans owned by VA and contains information for over 20 million Veterans. USVETS is produced by the Office of Enterprise Integration: Data, Governance and Analytics.

2. VADIR is the, an electronic repository of active and reserve military personnel, provided to VA by the Department of Defense’s Defense Manpower Data Center (DMDC).

Data gathered from VADIR and USVets, such as last known vital status, name, address, email address and phone number can change over time and will require updating prior to sample recruitment. Acxiom will be used to append the sample contact information:

3. Acxiom uses its unique databases to confirm and/or update the contact information for the sampled Veterans. Updating mailing addresses, phone numbers and email addresses improves the efficiency of the recruitment process and increases the likelihood that a representative sample of responses will be collected.
Response data will be collected via the Voxco survey administration tool.

4. The ASCEND system creates response data that will be collected directly from the individuals who choose to participate in the survey.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Using USVETS and VADIR to design a sampling frame to the ASCEND survey allows the study team to invite participation from members of the entire Veteran population, not just those who use VHA services. It also allows the study team to oversample key groups of Veterans who are known or believed to be at elevated risk for suicide (e.g., those who are females, not utilizing VHA services, recently separated, or rural). The ASCEND project has requested and been approved to use USVETS data through a VA Office of Data Governance & Analytics internal data sharing agreement. The ASCEND team will request VADIR data through the VA Digital Enterprise Service Collaboration Portal. USVETS and VADIR data will be transmitted electronically to the ASCEND team in the VA Informatics and Computing Infrastructure (VINCI).

To receive contact information updates from Acxiom, NORC must obtain from the VA (via secure file transfer protocol (SFTP)) a copy of the relevant contact information (including SSN) for only those Veterans included in the selected sample. As an alternative to SFTP, the ASCEND team intends to also use mailing as an option for data transfer. For mailing, the ASCEND team intends to United Parcel Service (UPS) Ground or United States Postal Service (USPS) Priority Mail for secure delivery service with tracking from pick-up to delivery in accordance with VA Directive 6609 and VA Handbook 6500 to securely mail VA PII data. The ASCEND team will be using the AEGIS Secure Key USB 2.0 (Part Number ASK3-480KB), which is a FIPS 140-2 Validated Removable Storage Device. The device password will be sent separately, via an encrypted VA email. The file will be accessed, and data downloaded immediately upon receipt of the device. Once the sample data has been accessed, the USB device will be re-encrypted and sent back to the VA, where it will be kept in a locked drawer behind locked office drawers.

The transferred file will then be converted into .csv format and uploaded to Acxiom via SFTP. Acxiom then searches its unique databases, using a proprietary algorithm, that associates information with the person being searched, and returns, if available, the best, last seen, address and phone number. Acxiom will have read-only access to the contact file and will not permanently store any information sent by NORC.
Voxco, an integrated survey administration and data collection platform, will be used to collect survey responses and will track response rate for targeted Veteran subgroups. Veterans will have three options to respond to the survey:

**Option 1** - Veterans will access the survey via the URL provided in the initial mailing. The URL will direct Veteran to a login page and Veteran will log into survey by entering a unique, randomly generated Study ID (e.g., consisting of random combination of characters and numbers that are in no way related to the Veteran’s PII [e.g., SSN, DOB, etc.]).

**Option 2** - Veterans can complete the survey on the phone after receiving a call from NORC or by calling a dedicated phone number. A trained NORC staff member will conduct the survey over the phone. NORC staff will enter survey responses into using Voxco’s CATI tool directly. NORC staff will have unique Voxco accounts.

For pilot data collection—Midway through the data collection period, Veterans will be mailed a hard copy of the survey instrument. They will have the option to complete the survey using pen and paper, and to mail the survey back to NORC using the included prepaid envelope. NORC staff will manually enter the survey responses into Voxco. Quality assurance and peer review procedures will be in place to ensure accurate and reliable data entry.

**1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?**

*Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.*

*If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose. This question is related to privacy control AP-2, Purpose Specification.*

Veteran SPI is collected and used to design and select a nationally representative sample of Veterans who will be invited to respond to the ASCEND survey. A selected sample is important to ASCEND’s research methods because it allows us to collect representative responses from key groups of Veterans who are known or believed to be at elevated risk for suicide (e.g., those who are females, not utilizing VHA services, recently separated, or rural). SPI is also used to contact Veterans in an effort to recruit them to participate in the survey.

**1.5 How will the information be checked for accuracy? How often will it be checked?**

*Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.*
If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract. This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Information will be checked for accuracy prior to recruitment, using Acxiom. After data collection and analysis is complete, response data will again be checked for accuracy in accordance with ASCEND’s data management plan. Key demographics such as age, gender, ethnicity, and age will be collected directly from the respondent as part of the research survey and compared to the expected demographic values from the sampling frame.

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect.

The legal authority in this project falls under Title 38, United States Code, Section 7301.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current? This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:
Privacy Risk: This systems/project has been determined to be of moderate risk, based on its
categorization as a “Major” system, without nation security impact. Further, loss of confidentiality,
integrity and availability carry financial and reputational damage, without loss to life or limb. Finally,
the negating of research accuracy/effectiveness may suffer in the case of security breach. The system has
been classified as a having “Moderate” impact if breached.

Mitigation: In mitigation of moderate risk, the project shall adhere to all applicable security controls and
ongoing patching recommendations. These controls include, but are not limited to: NIST, FIPS, STIG
and administrative oversight, as assessed and directed by appointed VA Security Officers. Any residual
risk found within the solution shall be tracked via POA&M and security relevant changes will be
recorded in eMASS. System administrators, engineers and developers shall report security relevant
changes and/or issues to the MTS Program Manager and SSO immediately. All site logging and auditing
standards shall be met, to include scanning, eradication effort and re-scan (until risk has been removed).
All high/zero-day risk shall be addressed immediately, and all else addressed as part of in place patch
management processes. FIPS approved encryption shall be used in protection of all CUI data, to ensure
its protection in travel and at rest. Finally, all accesses shall begin with an explicit deny all-to-all and
allowed only upon verified need and authorization. All additional mitigation requirements shall be
governed by on-site, VA NSOC and VA security professionals.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data
being used.

2.1 Describe how the information in the system will be used in support of the program’s business
purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained.
This question is related to privacy control AP-2, Purpose Specification.

SPI will be used to select a representative sample of potential respondents and to recruit those Veterans
for participation in the ASCEND research study. The overarching objective of the ASCEND project is to
develop a national survey of veterans that will:
1. Serve as a national surveillance system through recurring administration to document prevalence
   and trends over time in NF-SSDV among veterans
2. Provide estimates of the impact of risk and protective factors on NF-SSDV among veterans, with
   an emphasis on both individual and community level factors
3. Provide estimates of the impact of the COVID-19 pandemic on NF-SSDV among veterans

Information created and/or received by MTS and its subcontractors as part of the ASCEND contract will
be used only for the purposes of completed the tasks outlined in Contract #36C25919Q0310. Upon
completion of the contract, MTS shall return or destroy any and all PHI and other VA data created and/or
received from ASCEND study task. Data will be destroyed in compliance with VA 6500, VA 6500.1 –
Electronic Media Sanitization, and NIST 800-53 Media Protection (i.e., MP-6 Media Sanitization). No
such information will be retained by MTS unless retention is required by law or specifically permitted by
the VA.
The table below shows the data elements will be collected by the ASCEND system.

### List of Data Elements Collected

<table>
<thead>
<tr>
<th>Data element</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>First, middle and last name</td>
<td>Veteran identification</td>
</tr>
<tr>
<td>Veteran ID (SSN)</td>
<td>Veteran identification and location</td>
</tr>
<tr>
<td>Indicator for whether or not the person was living at the end of FY 2017</td>
<td>Recruitment (only living Veterans will be recruited for participation in ASCEND)</td>
</tr>
<tr>
<td>Full address</td>
<td>Mailing of recruitment materials</td>
</tr>
<tr>
<td>County of residence</td>
<td>Study community level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Urbanicity</td>
<td>Study community level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Telephone number</td>
<td>Recruitment</td>
</tr>
<tr>
<td>Email address</td>
<td>Recruitment</td>
</tr>
<tr>
<td>Date of birth</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Gender</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Ethnicity</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Race</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Transition status</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Maximum separation date</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Veteran status</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>VHA usage information</td>
<td>Study individual level risk factors for NF-SSDV, estimate the prevalence of NF-SSDV among Veterans</td>
</tr>
<tr>
<td>Years of service</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Retirement indicator</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Branch</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Rank</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Wars served in</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Character of service</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Components served in</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Branch of most recent separation</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
<tr>
<td>Benefits used</td>
<td>Study individual level risk factors for NF-SSDV</td>
</tr>
</tbody>
</table>

### 2.2 What types of tools are used to analyze data and what type of data may be produced?

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it 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? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used. This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Statistical analysis software will be used to analyze the data collected from the ASCEND surveys. Initial results shall provide reporting on prevalence of key survey outcomes (e.g., non-fatal SSDV prevalence overall and within key subgroups). Survey data will be merged with complementary clinical and non-clinical, individual-level and community-level datasets, for further analysis. However, survey data (ASCEND data) will not be entered into an individual’s existing medical record and will not be accessible to Government employees who make determinations about that individual.

In the event that a study team member has an interaction with a research participant that incidentally reveals that the individual is in distress or thinking of harming themselves or others, the study team will refer that individual to the appropriate emergency or crisis resource. Outside of these safety procedures, no action would be taken against or for an individual because of the data generated from the ASCEND study.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.
All employees with access to PII will undergo a background check prior to beginning work duties. Data in transit shall be protected each security boundary by firewalls, and all rulesets shall begin with an explicit deny all-to-all and only allow traffic that with verified need and authorization. To ensure protection against privacy breach, data in use shall be only be used by fully security trained individuals, with a roll-based account to access such data, and a well-defined business requirement to take action involving the data. Access to those with a need-to-know requirement to the data will be granted by supervisors, and the VA will have oversight of new user access requests. All user rights must be approved by the Project Director or delegate prior to access being granted. Managers are required to submit a user deactivation request for anyone removed from the project so that data access will be removed immediately. All data use and storage shall be continuously monitored, such that any anomalies are spotted and addressed quickly, by security engineers. Criteria, controls, and procedures for access to PII are documented in the ASCEND Project Plan (Contract Deliverable 4.1.2).

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

The following data elements/items will be retained within the ASCEND authorization boundary during the duration of survey and approved ATO determination.

- First, middle and last name
- Veteran ID (SSN)
- Indicator for whether person was living at the end of FY 2017 (or most recent FY available)
- Full address
- State name
- County name of residence
- Urbanicity (urban/rural)
- Urbanicity (urban/large rural/small rural/isolated)
- Telephone number
- Email address
- Date of birth
- Gender
- Ethnicity
- Race
- Transition status
- Maximum separation date
- Veteran status
- VHA usage information
- Years of service
- Retirement indicator
- Branch
- Rank
- Wars served in
- Character of service
- Components served in
- Branch of most recent separation
- Benefits used
- ASCEND survey response data

Study data will be maintained and destroyed in accordance with VA Records Control Schedule 10-1 and the VA Eastern Colorado Health Care System (ECHCS) Research Investigator Files Retention and Disposition Standard Operating Procedures.

Information created and/or received by MTS and its subcontractors as part of the ASCEND contract will be returned to the VA or destroy at the completion of the contract. No such information will be retained by MTS unless retention is required by law or specifically permitted by the VA.

3.2 How long is information retained?

_In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods._

_The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented._

_This question is related to privacy control DM-2, Data Retention and Disposal._

Records are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. If the Archivist has not approved disposition authority for any records covered by the system notice, the System Manager will take immediate action to have the disposition of records in the system reviewed and paperwork initiated to obtain an approved records disposition authority in accordance with VA Handbook 6300.1, Records Management Procedures. The VA Office of Policy and Planning (OPP) will publish an amendment to this notice upon issuance of NARA-approved disposition authority. The records may not be destroyed until VA obtains an approved records disposition authority. OPP destroys electronic files when no longer needed for administrative, legal, audit, or other operational purposes. In accordance with title 36 CFR 1234.34, Destruction of Electronic Records, “electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules.” All VA data will be handled as documented within associated security documents. Shared data will be returned to the VA once it is no longer needed for research purposes, when the system ATO expires, and/or at the conclusion of the research study.
Regarding media to be mailed to NORC, the data retention and media return process is detailed below. Data mailed to NORC is a copy of data that will remain held by the VA, and the below information does not apply to that original data.

**Mailed Data Receipt and Return**
Upon receiving media via mail, the recipient will notify the sender of receipt and open the file with the provided password. The recipient will return the media using the same mailing protocol within five (5) business days. USB device will be re-encrypted before return to the VA.

**Data/Media Storage**
Upon receiving the media device and when extend time is required to return the device back to VA possession, the authorized recipient(s) will securely store the device when not in use. Extend time consists of when the device is stored overnight, one day or more, and not in use, and will not exceed more than 5 business days. Additionally, the media device will not be out of sight/possession of the authorized recipient(s) during use. Authorized personnel from listed companies in the signed Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) document for the ASCEND information system will securely store the device in a lockable cabinet/drawer and will always keep the office/room locked when the device is not in use. The listed security measurements are in accordance with VA Handbook 6500 security control Media Storage (MP-4).

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.  
*This question is related to privacy control DM-2, Data Retention and Disposal.*

The ASCEND information system is not the system of records for the associated data. At no time are records being destroyed. Official approval is not required. Records are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. If the Archivist has not approved disposition authority for any records covered by the system notice, the System Manager will take immediate action to have the disposition of records in the system reviewed and paperwork initiated to obtain an approved records disposition authority in accordance with VA Handbook 6300.1, Records Management Procedures. OPP will publish an amendment to this notice upon issuance of NARA-approved disposition authority. The records may not be destroyed until VA obtains an approved records disposition authority. OPP destroys electronic files when no longer needed for administrative, legal, audit, or other operational purposes. In accordance with title 36 CFR 1234.34, Destruction of Electronic Records, “electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules.”

3.4 What are the procedures for the elimination of SPI?
Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

This question is related to privacy control DM-2, Data Retention and Disposal

SPI will be stored electronically by the contractor team for the duration of the ASCEND project. Once final data sets have been delivered to the VA and the contract tasks have been completed, electronic data will be destroyed by MTS and its subcontractors in accordance with contract deliverable 4.2.1 – Data Destruction Plan (to be finalized in option year 2).

The final data set records contained in this system are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. If the Archivist has not approved disposition authority for any records covered by the system notice, the System Manager will take immediate action to have the disposition of records in the system reviewed and paperwork initiated to obtain an approved records disposition authority in accordance with VA Handbook 6300.1, Records Management Procedures. OPP will publish an amendment to this notice upon issuance of NARA-approved disposition authority. The records may not be destroyed until VA obtains an approved records disposition authority. OPP destroys electronic files when no longer needed for administrative, legal, audit, or other operational purposes. In accordance with title 36 CFR 1234.34, Destruction of Electronic Records, “electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules.”

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy of using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Protections will be put into place to maintain the confidentiality of records and reduce risks to privacy. All electronic data will be stored in strict compliance with Colorado Multiple Institutional Review Board (COMIRB) and VA R&D standards. Specifically, electronic data will be stored behind the VA firewall in a VA shared drive or other VA system that maintains compliance with all VA security polices and regulations. Access to all electronic study files will be password protected and/or user-restricted to key study personnel. As a research system, ASCEND minimizes the use of PII wherever possible, throughout project tasks. NORC sampling specialists will assign study ID numbers to the selected sample once it has been drawn, and research participants will be identified only by this anonymous study ID wherever possible.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.
While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

**Principle of Minimization:** Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

**Principle of Data Quality and Integrity:** Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

**Privacy Risk:** There is a risk that information could be retained for longer than necessary which could result in the information being compromised or incorrectly disposed of.

**Mitigation:** The records contained in this system have not been scheduled and will be kept indefinitely until such time as they are. The records may not be destroyed until VA obtains an approved records disposition authority from the Archivist of the United States.

### Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

**4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?**

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

**Internal Sharing Systems**

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared /received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Data Governance and Analysis (DGA) - USVets</td>
<td>Requested data will be used as a sampling frame with which to draw a representative sample of Veterans to survey for ASCEND.</td>
<td>SPI, including: First Name, Last Name, Middle Name, Veteran ID (or other unique identifier), Indicator for whether person was living at the end of FY 2017 (or most recent FY available), Full Address, State name, County name of residence, Urbanicity (urban/rural), Urbanicity (urban/large rural/small rural/isolated), Telephone Number, Email Address, Date of Birth, Gender, Ethnicity, Race, Transition Status, Maximum separation date, Veteran Status, VHA usage information, Years of service, Retirement Indicator, Branch, Rank, Wars served in, Character of Service, Components served in, Branch of most recent separation, Benefits used, Benefits used 2 years prior to most recent year available, Benefits used 1 year</td>
<td>SFTP transfer push to VINCI, protected by multiple factors of actor and hardware authentication</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared /received with the specified program office or IT system</td>
<td>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>VADIR</td>
<td>VADIR will be used as a supplement to the USVETS sampling frame, specifically to identify Veterans who have been recently discharged between the time of the last USVETS update and the date of the data request.</td>
<td>SPI, including: First Name, Last Name, Middle Name, Veteran ID (or other unique identifier), Indicator for whether person was living at the end of FY 2017 (or most recent FY available), Full Address, State name, County name of residence, Urbanicity (urban/rural), Urbanicity (urban/large rural/small rural/isolated), Telephone Number, Email Address, Date of Birth, Gender, Ethnicity, Race, Transition Status, Maximum separation date, Veteran Status, VHA usage information, Years of service, Retirement Indicator, Branch, Rank, Wars served in, Character of Service,</td>
<td>The ASCEND team will request VADIR data through the VA Digital Enterprise Service Collaboration Portal. VADIR data will be transmitted electronically to the ASCEND team in VINCI.</td>
</tr>
</tbody>
</table>
4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.

This question is related to privacy control UL-1, Internal Use.

Privacy Risk: There is a risk that data could be shared with VA users who do not have a need-to-know requirement to access the data.

Mitigation: Data shall only be accessible by VA employees/WOCs that have a roll-based requirement to access data for research purposes. Protections will be put in place to maintain the confidentiality of records and reduce risks to privacy. All electronic data will be stored in strict compliance with Colorado Multiple Institutional Review Board (COMIRB) and VA R&D standards. Specifically, electronic data will be stored behind the VA firewall in a VA shared drive or in another system that maintains compliance with all VA security policies and regulations. Access to all electronic study files will be password protected and/or user-restricted to key study personnel. As needed, the study PI (Claire Hoffmire) will consult with the VA ECHCS Privacy Officer and Information Security Officer through VA R&D on data security matters. All study personnel will meet human subject’s protection and other training requirements, per COMIRB approval, as well as secondary approval from the local VA R&D.
Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Note: This question is #6 and #7 in the Privacy Threshold Analysis.
Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

External Sharing Systems

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORC at the University of Chicago</td>
<td>NORC will receive the ASCEND sample to conduct recruitment and data collection.</td>
<td>Controlled unclassified information</td>
<td>DUA, MOU/ISA</td>
<td>Site-to-site VPN and SFTP or via mail</td>
</tr>
<tr>
<td>Acxiom</td>
<td>NORC will use Acxiom to update Veteran contact information for the purposes of</td>
<td>Full name, SSN, mailing address, phone number, DOB</td>
<td>NDA, DUA</td>
<td>Secure Web-Portal</td>
</tr>
<tr>
<td><strong>List External Program Office or IT System information is shared/received with</strong></td>
<td><strong>List the purpose of information being shared/received/transmitted with the specified program office or IT system</strong></td>
<td><strong>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</strong></td>
<td><strong>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</strong></td>
<td><strong>List the method of transmission and the measures in place to secure data</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>recruiting more efficiently.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PressAmerica</td>
<td>PressAmerica will mail recruitment materials and incentives to Veterans</td>
<td>Full name, mailing address, study ID</td>
<td>PressAmerica has project specific DUA with NORC/MTS</td>
<td>Secure Web-Portal</td>
</tr>
<tr>
<td>MTS Technical Support Desk</td>
<td>MTS will collect the full name, phone number, and current location (for safety purposes) of Veterans calling into the study help desk phone number. For Veterans emailing the study help email address, MTS will collect the email address and share a log of the interaction with the VA. Lastly, MTS receives study ID numbers for the purpose of data entry for paper survey responses.</td>
<td>Full name, current location, email address, phone number, study ID</td>
<td>MOU/ISA, BAA</td>
<td>The MTS support desk will receive information disclosed by Veterans over the phone. Coordination communications between the MTS support desk and NORC CATI interviewers will not contain any patient identifiers.</td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

N/A

### 5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.
Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments. Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Privacy Risk: There is a moderate risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: All shared PII shall be authorized for release, as governed by project management, for the purpose of use in identifying most current contact information for study subjects. All logging and auditing shall be:

- Reviewed daily, for errors, inconsistency and anomalies
- Limit in viewers (for audit trails) to those with a job-related need and current privileged access
- User access control and authentication is discussed in section 8.1
- Protected from unauthorized modifications
- Promptly backed-up to a centralized log server or media that is difficult to alter
- Subject to file integrity monitoring/change detection software, to ensure that existing log data cannot be changed without generating alerts (although new data being added must not cause an alert)

Data Mailing

In accordance with VA Directive 6609 and VA Handbook 6500, the electronic media (e.g. thumb drive) containing VA PII data will be secured with a password that is sent to the recipient in a separate email. The data will be mailed with a tracking service. A notice sheet containing language that explains that there are penalties for violations of the Privacy Act and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule will accompany the mailing. The sender will also notify the recipient via email that the package is underway.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.
If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Applicable authority for ASCEND is under the following SOR’s - Veterans Affairs/Department of Defense Identity Repository (VADIR)—VA” (138VA005Q), Health Program Evaluation SOR# 107VA008B; Non-Health Data Analyses and Projections for VA Policy and Planning SOR # 149VA008A; Veterans, Service Members, Family Members, and VA Beneficiary Survey Records SOR # 43VA008.

In addition, recruitment letters and consent information inform Veterans of their right to consent to participate in the study or decline to provide information.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.

This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

Invited Veterans may decline to participate in ASCEND at any time by calling or emailing the study help desk. Recruitment letters will include a consent postcard that clearly explains voluntary participation and the Veteran’s right to decline to provide information. The decision whether or not to participate will have no effect on the Veterans access to benefits, current or future clinical care.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?

This question is related to privacy control IP-1, Consent

Individuals consent only to the use of their information for research purposes. There are no other uses of the ASCEND information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.
Consider the following FIPPs below to assist in providing a response:

**Principle of Transparency:** Has sufficient notice been provided to the individual?

**Principle of Use Limitation:** Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

**Privacy Risk:** There is a risk that individuals will be unaware that their information was contained in the sampling frame databases.

**Mitigation:** Individuals consent only to the use of their information for research purposes. There are no other uses of the ASCEND information. Notice was given to the general public in the Federal Register on the following SORNs:


**Section 7. Access, Redress, and Correction**

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.

7.1 **What are the procedures that allow individuals to gain access to their information?**

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency’s FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency’s procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Data collection for this survey is a one-time process. While a participant is in the process of completing a survey (either over the phone, on the web, or using a pen and paper), he/she may change the answers to his/her survey, but once a survey is submitted, the survey is locked, and the participant may not revisit the survey, or the information submitted.
7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Data collection for this survey is a one-time process. While a participant is in the process of completing a survey (either over the phone, on the web, or using a pen and paper), he/she may change the answers to his/her survey, but once a survey is submitted, the survey is locked, and the participant may not revisit the survey, or the information submitted.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.

Survey data may not be corrected by participant after submission.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

Veterans will not be able to edit their answer choices once they have completed the survey.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?
Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge? This question is related to privacy control IP-3, Redress.

Privacy Risk: As this is a research project, there is no process for access, redress and correction of an individual’s record.

Mitigation: Information gathered will not be used to identify any specific Veterans. Survey responses will be used for research purposes only and will not impact clinical care or eligibility for any community or VA services.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Describe the process by which an individual receives access to the system.

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

There are five types of users for the ASCEND system:

1. Invited participants - Veterans may log on to complete the ASCEND survey by visiting a public-facing website and entering their Study PIN number. The Veteran will have “write-only” access to the system and will not have access to any PII within the ASCEND system.

2. Technical support staff – will have “write-only” access to the ASCEND system, through the public-facing website, to enter data from returned paper surveys. Technical support staff will also have access to PII (email address, name, current location) as provided by Veterans who call or email the support desk.

3. NORC Interviewers/Operators and Managers – Call Center Interviewers/Operators perform phone based interviews with respondents. Each case to be worked is added to the Interviewer/Operator case load once his/her workstation appears as available (i.e. technical security controls built into the software prevent interviewers/operators from selecting which case[s] they prefer to work on). Call Center Managers review cases to assure quality and
accuracy, but do NOT interact with respondents (except to manage customer service incidents/issues).

a. Call Center Interviewer/Operator
   i. Secure card key access to area
   ii. User ID (Active Directory)
   iii. Password
   iv. Upon acceptance the password/passphrase, the VOXCO system returns an authentication code via telephony, which must be entered at prompt to complete authentication

b. Call Center Case Managers
   i. Working from within the manned/secured call station:
      1. Secure card key access to area
      2. User ID (Active Directory)
      3. Password
   ii. Working from a managed external workstation (managed, patched and updated by NORC):
      1. VPN access (via hardware certificate)
      2. User ID (Active Directory)
      3. Password
      4. Authentication code (sent to mobile device and entered into the system)
      5. Re-enter User ID (Active Directory)
      6. Re-Enter Password

4. NORC Statisticians – have access to the ASCEND system, working from a managed external workstation (managed, patched and updated by NORC):
   i. VPN access (via hardware certificate)
   ii. User ID (Active Directory)
   iii. Password
   iv. Authentication code (sent to mobile device and entered into the system)
   v. Re-enter User ID (Active Directory)
   vi. Re-Enter Password

In addition, these users have access to the ASCEND data set on the VA network, through WOC appointments obtained in 2009 through the VA ECHCS MIRECC. When accessing the VA network though Citrix using PIV authentication, NORC statisticians act as VA users (user type #5, listed below).

Lastly, NORC statisticians access sample data mailed via USB removable drive for the purposes of transferring the data from the USB drive to the NORC secure server. They will be permitted to receive, open, decrypt, and return the removable media. They will decrypt the removable media using a password securely emailed to their VA email address, which is accessed via PIV authentication.

5. VA Users – Once the ASCEND data set has been returned to the VA (following data collection and analysis), the data will live on the VA Rocky Mountain MIRECC research data drive where it can be accessed by VA users, who have access to the file folder where it is shared, using PIV authentication.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality
agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Technical support staff and NORC interviewers/managers (user types 2 and 3 in section 8.1) are VA contractor staff. While MTS will govern all changes, updates and patch management of the system, NORC shall be solely responsible for the design and maintenance of technical components of their system. Likewise, MTS shall manage and maintain all systems required to perform and monitor helpdesk functions. All contractor staff with access to PII will be required to sign a privileged access agreement.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.
This question is related to privacy control AR-5, Privacy Awareness and Training.

NORC CATI interviewers complete the following training modules: NORC code of ethics, data security and data integrity, confidentiality, privacy and HIPAA. MTS call center staff complete the following training modules: Attestation/Acknowledgement of terms within Data Use Agreements, Data classifications and classified data handling (including HIPAA training), Employee Codes of Conduct, Privileged Access Agreements, Identifying and Reporting Cyber Incidents, Annual Security Refresher Briefing. In addition, ASCEND VA users and users with access to the VA site-to-site VPN connection will complete OI&T security and privacy awareness training on a yearly basis.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).
Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.

If No or In Process, provide your Initial Operating Capability (IOC) date.

Authority to Operate (180 day) was granted 04-Jun-2020. System is classified as a moderate impact system.
# Section 9. References

Summary of Privacy Controls by Family

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Authority and Purpose</td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td>Accountability, Audit, and Risk Management</td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td>Data Quality and Integrity</td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td>Data Minimization and Retention</td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td>Individual Participation and Redress</td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td>Security</td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td>Transparency</td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td>Use Limitation</td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>ID</td>
<td>Privacy Controls</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

CHRISTIAN D LOFTUS 222466
Digitally signed by CHRISTIAN D LOFTUS 222466
Date: 2020.11.13 12:39:33 -05'00'

Privacy Officer, Christian Loftus

Tristan M. Carroll 1758903
Digitally signed by Tristan M. Carroll 1758903
Date: 2020.11.13 12:04:18 -06'00'

Information Security Systems Officer, Mark McGee or Tristan Carroll

Melanie S Reed 1367266
Digitally signed by Melanie S Reed 1367266
Date: 2020.11.13 08:35:00 -07'00'

Information System Owner, Melanie Reed
APPENDIX A-6.1

VADIR (SOR # 138VA005Q) and USVETS each have applicable system of records notices. USVETS falls under three active SORs: Health Program Evaluation SOR# 107VA008B; Non-Health Data Analyses and Projections for VA Policy and Planning SOR # 149VA008A; Veterans, Service Members, Family Members, and VA Beneficiary Survey Records. SOR # 43VA008.

ASCEND Invitation Letter

ASCEND Survey Invitation Letter 1

< Insert date >

Dear <Insert name >:

We are writing to you on behalf of the Department of Veterans Affairs (VA) because we need your help preventing Veteran suicides by participating in a one-time survey. Regardless of whether you have experienced thoughts of suicide yourself, you can help us shape future healthcare, research, and policy by increasing knowledge about suicide and how to prevent it. It is critical that we hear from Veterans who served at different times, who have had different experiences with the military (whether positive or negative), and regardless of whether they have ever used VA services. To understand this problem and help reduce suicides among Veterans, we need to hear from as many selected Veterans as possible, regardless of whether you have personally experienced suicidal thoughts.

The survey that you have been randomly selected to participate in is called Assessing Social and Community Environments with Notional Data (ASCEND) for Veteran Suicide Prevention. The goal of the ASCEND research study is to learn more about how many Veterans have experienced suicidal thoughts and behaviors and how many have not, what increases Veterans' risk for suicide, and what protects Veterans from experiencing suicidal thoughts and behaviors. ASCEND is being conducted by the VA Rocky Mountain Mental Illness Research, Education and Clinical Center (MIRECC) for Veteran Suicide Prevention, along with Minuteman Technology Services, a Veteran-owned small business, and NORE at the University of Chicago.

Your participation in this survey is completely voluntary, and should you choose to participate, you can stop the survey at any time. If you participate, your responses will always remain confidential and secure; your participation will not have any impact on your ability to receive VA care, benefits, or services. Information gathered will be used to improve suicide prevention practices for Veterans but will never be used to identify any specific Veterans at increased risk for suicide. We estimate that the survey will take an average of 45 minutes to complete.

https://ascend.va.gov

Version Date: February 27, 2020
Page 39 of 42
ASCEND Survey Invitation Letter 2

ASCEND
For Veteran Suicide Prevention

We have enclosed $1 as a token of our appreciation for your participation. Additionally, you will receive $5/$10/$20 upon completion of this survey. If you wish, you can choose to decline to receive this compensation and instead have the money donated to one of the below three charities:
1. The Tragedy Assistance Program for Survivors (TAPS)
2. The National Veterans Foundation (NVF)
3. The American Foundation for Suicide Prevention (AFSP)

To complete the survey online, enter the URL below in your browser, followed by your unique PIN and access code pair. The online survey has been designed to be completed on a computer, tablet, or smartphone.

Survey URL: https://mksurvey.norc.org/ASCEND
Your Personal PIN: [PIN]

If you prefer to complete the survey over the telephone, please call xxx-xxxx-xxxx, between the hours of 8:00 am to 8:00 pm EST/EDT (Monday through Friday, except for holidays).

If you have questions about the study, please visit our website at <VA Web Site> or contact us at xxx-xxxx-xxxx or <study email address>.

If you do not wish to participate in this study, please contact the ASCEND research team at xxx-xxxx-xxxx or <insert study email address>.

If we do not hear from you, we may contact you again by mail and/or by phone.

Thank you for your time and service.

Sincerely,

Claire Hoffmire, Ph.D. and Lindsey Monteith, Ph.D. (Principal Investigators)
Rocky Mountain MIRECC for Veteran Suicide Prevention
Rocky Mountain Regional VA Medical Center
1700 N Wescott St.
Aurora, CO 80045

https://ascend.va.gov
NORC Voxco SQL databases are built on a hierarchy of technologies and security. This document outlines who is responsible for security at each layer and what mechanism are used to implement the security. All hardware and software are managed by NORC staff. There are no shared infrastructure or managed services in the NORC environment.

Microsoft Voxco SQL hierarchy

<table>
<thead>
<tr>
<th>Ascend Database</th>
<th>SQL Databases</th>
<th>SQL Databases</th>
<th>SQL Databases</th>
<th>SQL Databases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Clustering</td>
<td>Microsoft SQL Clustering</td>
<td>Microsoft SQL Clustering</td>
<td>Microsoft SQL Clustering</td>
<td>Microsoft SQL Clustering</td>
</tr>
<tr>
<td>Microsoft SQL Instances</td>
<td>Microsoft SQL Instances</td>
<td>Microsoft SQL Instances</td>
<td>Microsoft SQL Instances</td>
<td>Microsoft SQL Instances (Failover node)</td>
</tr>
<tr>
<td>Virtual Server</td>
<td>Virtual Server</td>
<td>Virtual Server</td>
<td>Virtual Server</td>
<td>Virtual Server</td>
</tr>
<tr>
<td>VMWare Hypervisor</td>
<td>VMWare Hypervisor</td>
<td>VMWare Hypervisor</td>
<td>VMWare Hypervisor</td>
<td>VMWare Hypervisor</td>
</tr>
</tbody>
</table>

VMWare Hypervisor

All SQL databases are built on the VMWare hypervisor foundation. All hardware is owned and managed by NORC. The hypervisor level is managed by the NORC server team. Security of the hypervisor is managed through Active Directory and local security groups.

Virtual servers

All virtual servers are created by the VMWARE hypervisor. The virtual servers are managed by NORC server teams. The server team are the only personnel that can create a virtual server. The virtual server security is managed through Active Directory security groups.

Windows Operating System

Windows SQL servers are dedicated SQL servers. They do not support any other applications. The SQL servers are Windows 2012 or 2016 operating systems. The Windows operating system are managed by the NORC server team. The operating systems are configured according to the Center for Internet Security(CIS) configuration standards. Access to the server is managed through Active Directory groups. These Active Directory groups are monitored and alerts are sent out for any changes to these groups.