CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)	
Introduction: OATI issues mostly Client Authentication Certificates to the Wholesale, Retail and Smart Grid Energy Industries which are used usernames and passwords to authenticate to web and mobile applications. Less than 1% of active certificates are used for Server Authentication. OATI operates a single public root and a single subordinate CA. The subordinate CA is internally operated.	
1) CA's Legal Name:	Open Access Technology International, Inc.
2) Root certificates being evaluated and full CA hierarchy: .	***SHA-1 Fingerprint:*** 4B:6B:D2:D3:88:4E:46:C8:0C:E2:B9:62:BC:59:8C:D9:D5:D8:40:13 ***SHA-256 Fingerprint:*** 7A:77:C6:C6:1E:EE:B9:AA:65:C4:EA:41:0D:65:D8:95:B2:6A:81:12:32:83:00:9D:B1:04:B4:8D:E8:0B:24:79 ***CA Hierarchy:*** One internally-operated root CA called "OATI WebCARES Root CA" and one internally-operated intermediate CA called "OATI webCARES Issuing CA". ***Summary***: The internally-operated subordinate CA signs certificates to be used for both Server Authentication and the optional Client Side Authentication within an SSL/TLS session. ***Root Certificate Download UR:*** http://www.oaticerts.com/repository/OATICA2.crt ***Externally Operated SubCAs:*** OATI does not have and does not allow externally operated SubCAs. ***Cross Signing***: OATI's webCARES Root Certificate Authority does not cross-sign with any other root certificates. ***Technical Constraint on 3rd party Issuer:*** OATI has Local Registration Authorities (LRAs). The subject of each certificate issued by OATI's Local Registration Authorities is pre-determined by the organizational data submitted and verified during the Subscriber Identification and Verification Procedure (SIVP). Pre-filled fields and form dropdowns provide the technical constraints necessary to prevent issuance of certificates with misleading or incorrect information.
3) List the specific version(s) of the BRs used:	BR version 1.4.4, https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.4.4.pdf
4) CA's documents, certificates and URLs:	1. Current OATI Certification Practice Statement v 3.2 (CPS): http://www.oaticerts.com/repository/OATI-webCARES-CPS.pdf 2. Business Representative Application Form (BRAF): http://www.oaticerts.com/repository/webCARES%20Business%20Representative%20Application%20Form.pdf 3. OATI Root Certificate: http://www.oaticerts.com/repository/OATICA2.crt 5. OATI 2013 Issuing Authority Certificate: http://www.oaticerts.com/repository/OATIIA2013.crt
5) Next version of CPS:	Annually or when dictated by changes to industry standards.
6) Notes:	1. Glossary items from the CPS were listed below only when they help clarify subsequent CPS text.
	2. This table shows the differences between sections in OATI's CPS and RFC 3647.

OATI CPS	***Section***	***RFC 3647***
Acronyms and Glossary	1	Introduction
OATI webCARES	2	Publication and Repository
OATI webCARES Digital Certificates Practice and Procedures	3	Identification and Authentication
Facility, Management, and Operational Controls	4	Certificate Life-Cycle Operational Requirements
Technical Controls	5	Facilities, Management, and Operational Controls
External Party Obligations	6	Technical Security Controls

Certificate, CRL, and OCSP Profiles	7	Certificate, CRL, and OCSP Profile
Legal Information	8	Compliance audit
OATI 24x7x365 Customer Support	9	Other Business and Legal Matters
Compliance Audits	10	
Copyright Statement	11	

3. CPS Section 3.2.1 “webCARES Application Process” and CPS Section 3.2.1.1 “Identity Proofing Requirements” are listed here to shorten and organize this review as they are referenced frequently in the table below.

CPS Section 3.2.1 webCARES Application Process

OATI customers will designate employees to perform the roles of SO, BSO, and AO. The SO shall complete and return a notarized BRAF to OATI as part of OATI’s SIVP.

OATI webCARES personnel follow an extensive SIVP prior to issuing Digital Certificates. The SIVP begins with an applicant completing the BRAF. The BRAF requires an applicant to provide detailed information about themselves, their company, domain names owned by the applicant, and the purpose for which the Digital Certificate will be used.

Upon receipt of a completed BRAF, OATI webCARES personnel continue the SIVP that includes steps to ensure that the organizational information to be included in the certificate has been verified, the identity of the applicant (the person requesting the certificate) has been verified, if the request is on behalf of an organization, then the authority of the applicant to make that request has been verified, and the identity and organization validation are tied together so that there is reasonable assurance that someone cannot submit forged or stolen documents and receive a certificate in his/her name (or that of a company). The application process contained in Section 3.2, including the various verification and identity proofing processes, apply to all applications received for webCARES Digital Certificates for any applicable use including: Server and Client Authentication, and Secure E-mail . The SIVP includes, but is not limited to:

- Calling the applicant’s contacts provided on the BRAF.
- Verifying the Data Universal Numbering System (DUNS) number provided, and researching the applicant’s company.
- Verifying applicant control over e-mail addresses that will be included in certificates by sending an e-mail and requiring a response from the receiver.

CPS Section 3.2.1.1 Identity Proofing Requirements

To conform to SIVP, identity verification shall be performed prior to the issuance of all OATI webCARES Digital Certificates. The authentication requirements to be used are defined by NIST SP800-63 version 2.0 section 5.3.1 General Requirements per Assurance Level.
To meet the requirements for the Basic assurance level, SOs can verify the identity of Subscribers in one of three ways.

1. The SO can validate a Subscriber’s identity in person by having the Subscriber present a valid and current government issued picture ID.

2. The SO can validate a Subscriber’s identity remotely through the Subscriber’s presenting a valid and current government issued picture ID and a financial account number that can be confirmed.

3. SO’s issuing OATI webCARES Digital Certificates to internal employees may perform identity verification through their company’s Human Resources background screening performed upon employment, a corporate issued picture ID and/or an online process where notification is sent via the distribution channels normally used for sensitive, personal communications.

4. Per CPS Acronyms SIVP = Subscriber Identification and Verification Procedure

BR Section Number	*Doc. & Sect. #*	*Explain how the CA's listed documents meet the requirements of each BR section.*
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	Compliant. For additional details please see appropriate CPS sections below.	
1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	Compliant. For additional details please see appropriate CPS sections below.	
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.	Compliant. CPS Section(s): 1.2, 2.5, 3.3.1	In CPS Local Registration Authority (LRA) is equivalent to an Enterprise RA (BR 1.3.2) who is "an employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization." The titles of Security Officer (SO), Backup Security Officer (BSO) and Unaffiliated Individual are also used in our CPS. All five roles; LRA, Enterprise RA, SO, BSO and Unaffiliated Individual represent the same legal entity and can be used interchangeably. CPS section 1.2 Glossary: Security Officer: A person contractually responsible for issuing and managing OATI webCARES Digital Certificates within an Organizational Unit or an Unaffiliated Individual with access to the OATI webCARES solution. Each individual designated as a SO must have his/her identity verified using the OATI SIVP before he/she will be granted access the OATI webCARES system or receive an OATI webCARES Digital Certificate. See also Local Registration Authority. Backup Security Officer: A person designated within an organization to take on the duties and responsibilities of SO in the absence of the primary SO. Local Registration Authority: A delegation of the RA functions by the CA to external registration authorities that may or may not be part of the same legal entity as the CA. See also Security Officer. Unaffiliated Individual: A person applying for access to the OATI webCARES system for the purpose of issuing and managing OATI webCARES Digital Certificates for his or her personal

BR Section Number	Doc. & Sect. #	Explain how the CA's listed documents meet the requirements of each BR section.
		use. An Unaffiliated Individual who is approved through the OATI SIVP and is given access to the OATI webCARES system will be termed a Security Officer, and will assume all duties and obligations of a LRA. CPS section 2.5 Registration Authorities: The OATI Registration Authority (RA) may delegate RA duties to Local Registration Authorities (LRAs). The RA and/or LRA, where applicable, is responsible for performing the OATI webCARES SIVP (Subscriber Identification and Verification Procedure) or other acceptable methods of identity verification in conformance with applicable standards. This procedure is documented and ensures that OATI issues webCARES Digital Certificates to entities that are verified using commercially reasonable industry practices and procedures. CPS section 3.3.1 Security Officer/Local Registration Authority: The role of SO, otherwise known as a LRA, is mandatory for every organization or entity subscribing to the OATI webCARES system. A SO will be responsible for managing the Digital Certificates within his or her Organizational Unit. A SO will be responsible to use the OATI webCARES system to perform the SO's duties and responsibilities described in this CPS. A SO is delegated the right to serve as a LRA. The SOs duties and contractual obligations include issuing, revoking, renewing, tracking OATI webCARES Digital Certificates for his or her End Users, and revoking OATI webCARES Digital Certificates. A SO will be provided personal access to the OATI webCARES system to perform his or her role. All SOs must follow CA Browser Baseline Requirements or risk revocation of their Digital Certificate.
2.1. Repositories Provide the direct URLs to the CA's repositories	Compliant. CPS Section(s): 3.4.9, 5.1.2, 7.4, 8.1	https://www.oaticerts.com/repository/ CPS Section 3.4.9 CRL and OCSP Revocation Data CPS Section 5.1.2 CA Public Key Delivery to Users CPS Section 7.4 OATI CRL Publishing CPS Section 8.1 Conditions of Usage of the webCARES Repository and Website
2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." Copy the specific text that is used into the explanation in this row. (in English) AND List the URLs to the three test websites for each root certificate under consideration, as per: "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly	Compliant. CPS Section(s): 4.2.2, 10.1	***BR Section 2.2 Paragraph 1:*** Our CPS section order is based on RFC 3647 when possible and NAESB WEQ-12 when required. All appropriate material is present in our CPS but the order does not strictly conform to RFC 2527 or 3647. See note #2 (above) for a table which shows the differences between sections in OATI's CPS and RFC 3647". OATI will seek to redo the order of our CPS to conform to RFC 3647 in the future. ***BR Section 2.2 Paragraph 2:*** Currently CPS Section 4.2.2 CAA Records states... "OATI does not review CAA Records."

BR Section Number	Doc. & Sect. #	Explain how the CA's listed documents meet the requirements of each BR section.
trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired."		However, effective as of 8 September 2017, section 4.2.2 of OATI's CPS will state OATI's policy or practice on processing CAA Records for Fully Qualified Domain Names; that policy shall be consistent with these Requirements. It shall clearly specify the set of Issuer Domain Names that the CA recognizes in CAA "issue" or "Issue wild" records as permitting it to issue. OATI will log all actions taken, if any, consistent with its processing practice. ***BR Section 2.2 Paragraph 3:*** CPS Section 10.1 External Audits "The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (CA/B Forum BRs), the NAESB WEQ-012, and the AICPA/CICA WebTrust Program for Certification Authorities (WebTrust). OATI receives annual audits by an independent external auditor to assess OATI's compliance with this CPS, CA/B Forum WebTrust, and WEQ-012 criteria. The audits cover OATI's systems, processes and procedures regarding the OATI webCARES Digital Certificate PKI operations, and its compliance with applicable guidelines and standards." ***BR Section 2.2 Paragraph 4:*** Test Web Pages with Subscriber Certificates that are (i) Valid: https://www.oaticerts.com (ii) Revoked: https://revoked.oaticerts.com (iii) Expired: https://expired.oaticerts.com
2.3. Time or frequency of publication. Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.	Compliant. CPS Section(s): 2.3, 10.1, 10.2	CPS Section 2.3 Certification Practice Statement Management The maintenance of the OATI Certification Practice Statement will be managed by the OATI Compliance Department and designees. The CPS is always publically available and will be reviewed at least annually and updated as necessary to reflect changes to applicable industry standards including, but not limited to, WEQ-12, webTrust and CABF Baseline Requirements. CPS Section 10.1 External Audits The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (CA/B Forum BR's), the NAESB WEQ-012, and the AICPA/CICA WebTrust Program for Certification Authorities (WebTrust). OATI receives annual audits by an independent external auditor to assess OATI's compliance with this CPS, CA/B Forum WebTrust, and WEQ-012 criteria. The audits cover OATI's systems, processes and procedures regarding the OATI webCARES Digital Certificate PKI operations, and its compliance with applicable guidelines and standards.

BR Section Number	Doc. & Sect. #	Explain how the CA's listed documents meet the requirements of each BR section.
		CPS Section 10.2 Internal Audits OATI also monitors adherence to its Certificate Policy, CA/B Forum, NAESB WEQ-012 and WebTrust requirements and strictly controls its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the webCARES Digital Certificates issued by OATI during the period commencing immediately after the previous self-audit sample was taken.
2.4. Access controls on repositories Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.	Compliant. CPS Section(s): 2.3	CPS Section 2.3 Certification Practice Statement Management The maintenance of the OATI Certification Practice Statement will be managed by the OATI Compliance Department and designees. The CPS is always publically available and will be reviewed at least annually and updated as necessary to reflect changes to applicable industry standards including, but not limited to NAESB WEQ-12, WebTrust, and CA/B Forum Baseline Requirements.
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, indicate how your CP/CPS meets the requirements in this section of the BRs.	Compliant. CPS Section(s): 1.1, 3.2.1, 3.2.1.1	CPS Section 1.1 Acronyms SIVP: Subscriber Identification and Verification Procedure CPS Section 3.2.1 webCARES Application Process CPS Section 3.2.1.1 Identity Proofing Requirements
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, indicate how your CP/CPS meets the requirements in this section of the BRs.	Not Applicable. CPS Section(s): 2.11	OATI does not allow DBA/Tradenames in any Subject fields. Note: Organization (O) and Organizational Unit (OU) fields are pre-populated with values during or SIVP vetting process and cannot be changed unless a modified BRAF is submitted. CPS Section 2.11 OATI Naming Authority The OATI NA coordinates the creation and issuance of DN for all certificates issued to SOs and End Users. OATI webCARES Digital Certificates issued within the OATI PKI will contain a unique X.500 DN. The DN assigned by the OATI NA will clearly identify the official Company Name, the Company's Entity code, the name of the End Entity or machine ID, and the e-mail address of the person responsible for the Digital Certificate, as applicable. By combining all of these elements into the DN, OATI assures that every DN assigned will be unique and will clearly identify the party using the Certificate.
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, indicate how your CP/CPS meets the requirements in this section of the BRs.	Compliant. CPS Section(s): 3.2.1	OATI uses option (d) "a method identified in BR Section 3.2.2.1 "A third party database that is periodically updated and considered a Reliable Data Source". CPS Section 3.2.1webCARES Application Process
3.2.2.4 Validation of Domain Authorization or Control Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's	Compliant. CPS Section(s): 3.2.1	CPS Section 3.2.1 webCARES Application Process "• Verifying Domain Name Ownership by making sure registration information returned from third party databases exactly match contract information OATI has for existing customers. If there is not an exact match domain ownership is done by making an agreed-upon change to their website."

BR Section Number	*Doc. & Sect. #*	*Explain how the CA's listed documents meet the requirements of each BR section.*
CP/CPS must clearly describe the acceptable methods of domain validation. It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.		
3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not Applicable.	OATI webCARES does not use this method.
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not Applicable.	OATI webCARES does not use this method.
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not Applicable.	OATI webCARES does not use this method.
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not Applicable.	OATI webCARES does not use this method.
3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not Applicable.	OATI webCARES does not use this method.
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Compliant. CPS Section(s): 3.2.1	See previous entry for "3.2.2.4 Validation of Domain Authorization or Control" 3.2.1 webCARES Application Process
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not Applicable.	OATI webCARES does not use this method.
3.2.2.4.8 IP Address If your CA uses this method of domain	Not Applicable.	OATI webCARES does not use this method.

BR Section Number	Doc. & Sect. #	Explain how the CA's listed documents meet the requirements of each BR section.
validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		
3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not Applicable.	OATI webCARES does not use this method.
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not Applicable.	OATI webCARES does not use this method.
3.2.2.5 Authentication for an IP Address If your CA allows IP Address to be listed in certificates, indicate how your CA meets the requirements in this section of the BRs.	Not Applicable.	OATI does not allow the use of IP Addresses.
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then indicate how your CA meets the requirements in this section of the BRs.	Not Applicable.	OATI does not allow the use of the wildcard character (*) and returns the message “The Common Name provided contains invalid characters.”
3.2.2.7 Data Source Accuracy Indicate how your CA meets the requirements in this section of the BRs.	Compliant. CPS Section(s): 3.2.1, 4.4	Databases maintained by OATI qualify as a Reliable Data Source because they contain reliable customer information obtained in non-CA operations. CPS Section 3.2.1 webCARES Application Process CPS Section 4.4 Records Retention Policy
3.2.3. Authentication of Individual Identity	Compliant. CPS Section(s): 3.2.1.1	CPS Section 3.2.1.1 Identity Proofing Requirements
3.2.5. Validation of Authority	Compliant. CPS Section(s): 3.2.1	CPS Section 3.2.1 webCARES Application Process
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	Not Applicable.	OATI’s PKI does not include any cross-certificates.
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	Compliant. CPS Section(s):	CPS Section 3.2.1.1 Identity Proofing Requirements “All Server Certificate requests are verified against Google’s Safe Browsing Lookup API to screen for High Risk Requests. Any requests identified by Google’s Safe Browsing Lookup API

BR Section Number	Doc. & Sect. #	Explain how the CA's listed documents meet the requirements of each BR section.
	3.2.1.1	as potentially containing malicious code or phishing attempts will be considered by OATI to be a High Risk Request, and as such, will be rejected and logged in the database."
4.1.2. Enrollment Process and Responsibilities	Compliant. CPS Section(s): 3.2.1	All certificate requests must come from verified Security Officers per CPS 3.2.1 webCARES Application Process. In addition all certificate subject fields, excluding Common Name and email address, are pre-populated with verified information obtained during the SIVP. If the Common Name and email address contain a FQDN it is verified per CPS Section 3.2.1 webCARES Application Process which states "…Verifying Domain Name Ownership by making sure registration information returned from third party databases exactly match contract information OATI has for existing customers. If there is not an exact match domain ownership is done by making an agreed-upon change to their website." Also, the digital signature on all certificate requests must be valid.
4.2. Certificate application processing	Compliant. CPS Section(s): 3.2.1	CPS Section 3.2.1 webCARES Application Process and CPS Section 3.2.1.1 Identity Proofing Requirements
4.2.1. Performing Identification and Authentication Functions Indicate how your CA identifies high risk certificate requests.	Compliant. CPS Section(s): 3.2.1.1	CPS Section 3.2.1.1 Identity Proofing Requirements
4.2.2. Approval or Rejection of Certificate Applications	Compliant. CPS Section(s): 3.2.1.1	CPS Section 3.2.1.1 Identity Proofing Requirements
4.3.1. CA Actions during Certificate Issuance	Compliant. CPS Section(s): 5.1.1	CPS Section 5.1.1 Key Pair Generation "OATI enforces multi-factor authentication for all accounts capable of directly causing certificate issuance. OATI webCARES CA key(s) are securely generated using Federal Information Processing Standards (FIPS) 140-2 Level 3 standards and take the applicable standard industry precautions to prevent the compromise or unauthorized use of the system. OATI Subscriber keys are securely generated after a multi-factor login to the webCARES system which includes a unique username, strong password and client authentication certificate."
4.9.1.1 Reasons for Revoking a Subscriber Certificate Reasons for revoking certificates must be listed in the CA's CP/CPS.	Compliant. CPS Section(s): 3.4.6	CPS Section 3.4.6 Conditions Requiring OATI webCARES Digital Certificate Revocation
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate	Not Applicable.	OATI does not have any external Subordinate CA's.
4.9.2. Who Can Request Revocation	Compliant. CPS Section(s):	CPS Section 3.4.5 OATI webCARES Digital Certificate Revocation

BR Section Number	*Doc. & Sect. #*	*Explain how the CA's listed documents meet the requirements of each BR section.*
	3.4.5, 3.4.7	"OATI webCARES can revoke an OATI webCARES Digital Certificate at any time. An SO can also revoke any OATI webCARES Digital Certificates they have issued to End Entities." CPS Section 3.4.7 Request for Revocation "An End Entity may request revocation of his/her/its OATI webCARES Digital Certificate at any time for any reason."
4.9.3. Procedure for Revocation Request	Compliant. CPS Section(s): 3.4.7	CPS Section 3.4.7 Request for Revocation "…The request must be written (i.e. email, fax, postal mail, etc.) and presented to the End Entity's SO, or OATI's Helpdesk, who approves the request and revokes the certificate via the webCARES User Interface…"
4.9.5. Time within which CA Must Process the Revocation Request	Compliant. CPS Section(s): 3.4.7	CPS Section 3.4.7 Request for Revocation "..The End Entity's SO, or OATI's Helpdesk, will begin investigation of the request for revocation within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria: 1. The nature of the reported problem. 2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber. 3. The entity making the complaint (for example, a complaint from a law enforcement official should carry more weight than a complaint from an End Entity alleging the information in her certificates is wrong). 4. Relevant legislation."
4.9.7. CRL Issuance Frequency	Compliant. CPS Section(s): 7.5	CPS Section 7.5 OATI CRL Publishing "The CRL published by the OATI webCARES Issuing CA has a validity period of twelve hours. The OATI webCARES Issuing CA publishes a new CRL prior to the expiration of the existing CRL, when a Certificate is revoked, and on regular intervals to assure availability. Both the OATI webCARES Root and Issuing CA CRLs are published in the OATI Repository at the following URL: www.oaticerts.com/repository."
4.9.9. On-line Revocation/Status Checking Availability	Compliant. CPS Section(s): 3.4.10	CPS Section 3.4.10 OCSP Responses "OATI webCARES OCSP responses conform to RFC6960 and/or RFC5019, are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. The OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960."
4.9.10. On-line Revocation Checking Requirements Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing erroneous return of "good" status.	Compliant. CPS Section(s): N/A	Visit: http://ocsp.oaticerts.com/ocsp

BR Section Number	*Doc. & Sect. #*	*Explain how the CA's listed documents meet the requirements of each BR section.*
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	Not Applicable.	OATI does not support OCSP stapling.
4.10.1. Operational Characteristics	Compliant. CPS Section(s): 3.4.8	CPS Section 3.4.8 Effect of Revocation "…The serial number of the revoked OATI webCARES Digital Certificate will be placed within the CRL within ten minutes of revocation and the serial number will remain on the CRL until after the end of the OATI webCARES Digital Certificate's validity period."
4.10.2. Service Availability	Compliant. CPS Section(s): 3.4.9, 9	CPS Section 3.4.9 CRL and OCSP Revocation Data "The CRL is published in the 24x7 OATI repository: http://www.oaticerts.com/repository/. OATI maintains webCARES CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions." CPS Section 9. OATI 24x7x365 Customer Support "The OATI Help Desk provides full support 24x7x365. Customers are encouraged to contact the OATI Help Desk by telephone, email, postal mail, and OATI application messaging systems. Operational emergencies must be reported by telephone to 763.201.2020….Critical Tickets are addressed within 30 minutes on a 24x7x365 basis."
5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS	Compliant. CPS Section(s):	Compliant. See individual entries below for CPS sections.
5.2.2. Number of Individuals Required per Task	Compliant. CPS Section(s): 4.1, 4.2, 4.2.1, 5.1.1.3	CPS Section 4.1 Physical Access "…Gaining physical access to the cryptographic module requires a minimum of two OATI trusted employees." CPS Section 4.2 Personnel Controls "…In addition, OATI employs a system of "separation of powers" by assigning webCARES personnel to no more than one critical position each, thus, ensuring that no single employee has the opportunity to compromise the system." "…Each employee assigned to a critical position will have appropriate personnel assigned and trained for backup purposes. Trusted roles are established to guarantee role separation." CPS Section 4.2.1 Trusted Roles "OATI webCARES operations are handled by multiple PKI personnel in trusted roles." CPS Section 5.1.1.3 Witnesses "OATI will engage an independent third party to witness and validate the key generation ceremony and/or OATI will video tape the ceremony."
5.3.1. Qualifications, Experience, and Clearance Requirements	Compliant.	CPS Section 4.2 Personnel Controls

BR Section Number	*Doc. & Sect. #*	*Explain how the CA's listed documents meet the requirements of each BR section.*
	CPS Section(s): 4.2	"OATI screens all employees working with or having access to the webCARES infrastructure. The personnel background investigation includes a criminal background check, employment and reference verification, and social security verification. In addition, OATI employs a system of "separation of powers" by assigning webCARES personnel to no more than one critical position each, thus, ensuring that no single employee has the opportunity to compromise the system. Each employee assigned to a critical position will have appropriate personnel assigned and trained for backup purposes. Trusted roles are established to guarantee role separation."
5.3.3. Training Requirements and Procedures	Compliant. CPS Section(s): 4.2	CPS Section 4.2 Personnel Controls "OATI provides all personnel performing information verification duties with skills-training and certification that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including this Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. In addition, those in the Administrator role receive training and certification on CA key lifecycle management including secure HSM operations. Each employee assigned to a critical position will have appropriate personnel assigned and trained for backup purposes."
5.3.4. Retraining Frequency and Requirements	Compliant. CPS Section(s): 4.2	CPS Section 4.2 Personnel Controls
5.3.7. Independent Contractor Controls	Not Applicable.	OATI does not delegate any of its CA Certificate issuance to third parties.
5.4.1. Types of Events Recorded	Compliant. CPS Section(s): 4.3, 4.4.1	CPS Section 4.3 Audit Logging Procedures CPS Section 4.4.1 Records Archive "OATI webCARES Auditor(s) will verify, package, transmit, and store physical archive information in accordance with the applicable industry standards for each assurance level. The contents of the OATI webCARES archive shall not be released except as required by law or applicable regulations and standards. Data to be archived include: • Record of CA Certificate Renewal and Reissuance • Other data or applications to verify archive contents • Compliance Auditor Reports • Any changes to audit parameters • Any attempt to delete or modify the log • Destruction of cryptographic modules • All Digital Certificate compromise notifications • Remedial action taken as a result of violations of physical security • Violations of the OATI CPS • Shipment receipt of cryptographic hardware (i.e., HSM modules, tokens, etc.) • All changes to trusted public keys • All Private Key relevant messages that are received by the system"
5.4.3. Retention Period for Audit Logs	Compliant.	CPS Section 4.4 Records Retention Policy

BR Section Number	*Doc. & Sect. #*	*Explain how the CA's listed documents meet the requirements of each BR section.*
	CPS Section(s): 4.4	"OATI retains, according to generally accepted industry practices, all records associated with OATI webCARES Digital Certificates after an OATI webCARES Digital Certificate is revoked or expires. Records will be retained in electronic format where applicable, all other retained records will be in a physical medium. Physical records will be retained in a secure fashion, for time periods required by applicable standards including, but not limited to, WebTrust, CA/B Forum BRs and NAESB WEQ-012."
5.4.8. Vulnerability Assessments	Compliant. CPS Section(s): 3.8.3	CPS Section 3.8.3 Incident Review and Notification "OATI maintains a Rick Assessment and Management Plan, Cyber Security Incident Response Plan and other processes to identify and remediate possible security risks. In the event of a security incident, OATI will notify Subscribers. OATI will notify law enforcement agencies as applicable based on the OATI Cyber Security Incident Response Plan."
5.5.2. Retention Period for Archive	Compliant. CPS Section(s): 4.4	CPS Section 4.4 Records Retention Policy "OATI retains, according to generally accepted industry practices, all records associated with OATI webCARES Digital Certificates after an OATI webCARES Digital Certificate is revoked or expires. Records will be retained in electronic format where applicable, all other retained records will be in a physical medium. Physical records will be retained in a secure fashion, for time periods required by applicable standards including, but not limited to, WebTrust, CA/B Forum BRs and NAESB WEQ-012."
5.7.1. Incident and Compromise Handling Procedures	Compliant. CPS Section(s): 3.8.1	CPS Section 3.8.1 Business Continuity following a Disaster "As part of OATI's Business Continuity Plan webCARES will notify Subscribers in the event of a disaster that damages the ACA and destroys copies of the ACA signature keys."
6.1.1. Key Pair Generation	Compliant. CPS Section(s): 5.1.1 – 5.1.1.3	CPS Section 5.1.1 Key Pair Generation "OATI enforces multi-factor authentication for all accounts capable of directly causing certificate issuance. OATI webCARES CA key(s) are securely generated using Federal Information Processing Standards (FIPS) 140-2 Level 3 standards and take the applicable standard industry precautions to prevent the compromise or unauthorized use of the system. OATI Subscriber keys are securely generated after a multi-factor login to the webCARES system which includes a unique username, strong password and client authentication certificate." CPS Section 5.1.1.1 Logging "OATI webCARES key generation activities will be logged in accordance with the applicable industry standards." CPS Section 5.1.1.2 Security "OATI webCARES key generation activities will take place in a physically secure environment." CPS Section 5.1.1.3 Witnesses "OATI will engage an independent third party to witness and validate the key generation ceremony and/or OATI will video tape the ceremony. "
6.1.2. Private Key Delivery to Subscriber	Compliant.	CPS Section 5.2 Private Key Protection

BR Section Number	*Doc. & Sect. #*	*Explain how the CA's listed documents meet the requirements of each BR section.*
	CPS Section(s): 5.2	"…Parties other than the Subscriber or the Subscriber's SO SHALL NOT archive the Subscriber Private Key without written authorization by the Subscriber sent to the Subscriber's SO or the OATI Helpdesk. If a Private Keys is generated on behalf of the Subscriber it is encrypted during transport to the Subscriber. If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key."
6.1.5. Key Sizes	Compliant. CPS Section(s): N/A	Root: Issued in 2008. Digest is SHA-1 with 4096 bit RSA keys in accordance with the criteria defined in Section 7.1.3. Sub CA/Issuer: Issued in 2013. Digest is SHA-256 with 4096 RSA. Subscriber: Digest is SHA-256 with 2048 RSA.
6.1.6. Public Key Parameters Generation and Quality Checking	Compliant. CPS Section(s): N/A	RSA Compliant.
6.1.7. Key Usage Purposes	Compliant. CPS Section(s): 5.3	CPS Section 5.3 Certificate Authority Key Usage "OATI Root CA key pairs are used for self-signed certificates to represent the Root CA itself and signing certificates for Subordinate CAs…"
6.2. Private Key Protection and Cryptographic Module Engineering Controls	Compliant. CPS Section(s): 5.5	CPS Section 5.5 Cryptographic Module Engineering Controls "OATI webCARES cryptographic modules for its CA private keys are validated to FIPS 140-2 Level 3 standards…"
6.2.5. Private Key Archival	Not Applicable.	OATI does not use Subordinate CAs or allow any archiving of its Subordinate CA private keys by a third parties.
6.2.6. Private Key Transfer into or from a Cryptographic Module	Not Applicable.	OATI does not use Subordinate CAs or allow transport of its Subordinate CA private keys to third parties.
6.2.7. Private Key Storage on Cryptographic Module	Compliant. CPS Section(s): 5.1.1, 5.5	CPS Section 5.1.1 Key Pair Generation "OATI enforces multi-factor authentication for all accounts capable of directly causing certificate issuance. OATI webCARES CA key(s) are securely generated using Federal Information Processing Standards (FIPS) 140-2 Level 3 standards and take the applicable standard industry precautions to prevent the compromise or unauthorized use of the system. OATI Subscriber keys are securely generated after a multi-factor login to the webCARES system which includes a unique username, strong password and client authentication certificate." CPS Section 5.5 Cryptographic Module Engineering Controls

BR Section Number	*Doc. & Sect. #*	*Explain how the CA's listed documents meet the requirements of each BR section.*
		"OATI webCARES cryptographic modules for its CA private keys are validated to FIPS 140-2 Level 3 standards. Subscribers must protect their Private Keys in accordance with the applicable guidelines on Private Key protection."
6.3.2. Certificate Operational Periods and Key Pair Usage Periods	Compliant. CPS Section(s): N/A	All of OATI's Subscriber Certificates have a validity period of 24 months.
6.5.1. Specific Computer Security Technical Requirements	Compliant. CPS Section(s): 5.1.1	CPS Section 5.1.1 Key Pair Generation "OATI enforces multi-factor authentication for all accounts capable of directly causing certificate issuance. OATI webCARES CA key(s) are securely generated using Federal Information Processing Standards (FIPS) 140-2 Level 3 standards and take the applicable standard industry precautions to prevent the compromise or unauthorized use of the system. OATI Subscriber keys are securely generated after a multi-factor login to the webCARES system which includes a unique username, strong password and client authentication certificate."
7.1. Certificate profile	Compliant. CPS Section(s): 7.1, 7.1.2.4	See previous responses to BR section 2.2. Publication of information and BR section 6.1.6. Public Key Parameters Generation and Quality Checking. Also OATI has always generated non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG. CPS Section 7.1 Certificate profile "OATI Certificates conform to RFC 5280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to RFC 5280 and in cases where stipulations of RFC 5280 and the applicable CA/Browser Forum Baseline Requirements differ, the Baseline Requirements notion will be adhered to." CPS Section 7.1.2.4 All Certificates "…Serial Numbers are generated with non-sequential numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG..."
7.1.1. Version Number(s)	Compliant. CPS Section(s): 7.1.1	CPS Section 7.1.1 Version number(s) "Subscriber certificates issued by OATI will be X.509 Version 3."
7.1.2. Certificate Content and Extensions; Application of RFC 5280	Compliant. CPS Section(s):	See individual sections below.
7.1.2.1 Root CA Certificate	Compliant. CPS Section(s): 7.1.2.1	CPS Section 7.1.2.1 Root CA Certificate.
7.1.2.2 Subordinate CA Certificate	Compliant.	CPS Section 7.1.2.2 Issuing CA Certificate

BR Section Number	Doc. & Sect. #	Explain how the CA's listed documents meet the requirements of each BR section.
	CPS Section(s): 7.1.2.2	
7.1.2.3 Subscriber Certificate	Compliant. CPS Section(s): 7.1.2.3	CPS Section 7.1.2.3 Subscriber Certificate
7.1.2.4 All Certificates	Compliant. CPS Section(s): 7.1.2.4	CPS Section 7.1.2.4 All Certificates
7.1.2.5 Application of RFC 5280	Compliant. CPS Section(s): 7.1.2.5	CPS Section 7.1.2.5 Application of RFC 5280
7.1.3. Algorithm Object Identifiers	Compliant. CPS Section(s): 7.1.3	CPS Section 7.1.3 Algorithm object identifiers “Effective 1 January 2016, OATI will not issue any new Subscriber certificates, Subordinate CA certificates or certificates to verify OCSP responses using the SHA-1 hash algorithm.”
7.1.4. Name Forms	Compliant. CPS Section(s):	See individual sections below.
7.1.4.1 Issuer Information	Compliant. CPS Section(s): 7.1.4.1	CPS Section 7.1.4.1 Issuer Information “The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the OATI certificate to support Name chaining as specified in RFC 5280, section 4.1.2.4.”
7.1.4.2 Subject Information	Compliant. CPS Section(s): 7.1.4.2	CPS Section 7.1.4.2 Subject Information “By issuing the Certificate, OATI represents that it followed the procedure set forth in this Certification Practice Statement to verify that, as of the Certificate’s issuance date, all of the Subject Information was accurate. OATI does not issue Certificates containing IP Addresses or Internal Names in the Subject Information.”
7.1.4.3 Subject Information - Subordinate CA Certificates	Compliant. CPS Section(s): 7.1.4.3	CPS Section 7.1.4.3 Subject Information – Subordinate CA Certificates “By issuing a Subordinate CA Certificate, OATI represents that it followed the procedure set forth in this Certification Practice Statement to verify that, as of the Certificate’s issuance date, all of the Subject Information was accurate.”
7.1.5. Name Constraints	Compliant. CPS Section(s): 7.1.5	CPS Section 7.1.5 Name constraints “OATI does not issue Subordinate CA Certificates to external parties and its internal Issuing CA is currently not technically constrained.”
7.1.6. Certificate Policy Object Identifier	Compliant.	See individual sections below.

BR Section Number	*Doc. & Sect. #*	*Explain how the CA's listed documents meet the requirements of each BR section.*
	CPS Section(s):	
7.1.6.1 Reserved Certificate Policy Identifiers	Not Applicable.	OATI webCARES does not use the optional Certificate Policy identifiers (2.23.140.1.2.1, 2.23.140.1.2.2, 2.23.140.1.2.3) as a means of asserting compliance with the BR's.
7.1.6.2 Root CA Certificates	Not Compliant. CPS Section(s): 7.1.6.2	When OATI renews its current Root Certificate it will ***not*** contain a Policy Extension. CPS Section 7.1.6.2 Root CA Certificates "No Stipulation."
7.1.6.3 Subordinate CA Certificates	Compliant. CPS Section(s): 7.1.6.3	OATI webCARES does ***not*** issue CA certificates to Subordinate CA that are not an affiliate of OATI. CPS Section 7.1.6.3 Subordinate CA Certificates "No Stipulation."
7.1.6.4 Subscriber Certificates	NOT Compliant. CPS Section(s): 7.1.6.4	OATI felt there was ongoing discussion regarding this requirement. OATI will fully implement this in the future by making sure our Subscriber Certificates contain one or more policy identifier(s) in the Certificate's certificatePolicies extension that indicates adherence to, and compliance with, these Requirements and may also assert one of the CABF reserved policy OIDs. (as we have done for the NAESB WEQ-12 Policies) CPS Section 7.1.6.4 Subscriber Certificates "No Stipulation."
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	Compliant. CPS Section(s): 8.12	CPS Section 8.12 Governing Law "This CPS shall be governed, construed, interpreted, and enforced in accordance with the laws of the state of Minnesota. Regardless of the place of residence or place of use of an OATI webCARES Digital Certificate, Subscribers hereby agree to a venue of Minnesota."
8.1. Frequency or circumstances of assessment	Compliant. CPS Section(s): 10.1	Note: OATI webCARES is technically Unconstrained and fully audited in line with all remaining requirements from this section. Note: OATI webCARES has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.1 so no pre-issuance readiness assessment is necessary. CPS Section 10.1 External Audits "The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (CA/B Forum CA/B BRs), the NAESB WEQ-012, and the AICPA/CICA WebTrust Program for Certification Authorities (WebTrust).

BR Section Number	Doc. & Sect. #	Explain how the CA's listed documents meet the requirements of each BR section.
		OATI receives annual audits by an independent external auditor to assess OATI's compliance with this CPS, CA/B Forum WebTrust, and WEQ-012 criteria. The audits cover OATI's systems, processes and procedures regarding the OATI webCARES Digital Certificate PKI operations, and its compliance with applicable guidelines and standards."
8.2. Identity/qualifications of assessor	Compliant. CPS Section(s): 10.1	OATI's Qualified Auditor is Schellman & Company, Inc. http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx CPS Section CPS Section 10.1 External Audits "…OATI receives annual audits by an independent external auditor to assess OATI's compliance with this CPS, CA/B Forum WebTrust, and WEQ-012 criteria…"
8.4. Topics covered by assessment	Compliant. CPS Section(s): 2.1	CPS Section 2.1 OATI webCARES Overview "…This CPS describes the practices that webCARES follows in issuing Digital Certificates in accordance with requirements found within the American Institute of Certified Public Accountants, Inc. (AICPA)/Canadian Institute of Chartered Accountants (CICA) WebTrust Program for Certification Authorities, and in accordance with other applicable industry standards."
8.6. Communication of results	Compliant. CPS Section(s): 2.3	OATI webCARES dos not assert one or more of the optional policy identifiers listed in Section 7.1.6.1. CPS Section 2.3 Certification Practice Statement Management "The CPS is always publically available and will be reviewed at least annually and updated as necessary to reflect changes to applicable industry standards including, but not limited to, WEQ-12, webTrust and CABF Baseline Requirements."
8.7. Self-Audits	Compliant. CPS Section(s): 10.2	CPS Section 10.2 Internal Audits "OATI also monitors adherence to its Certificate Policy, CA/B Forum BRs, NAESB WEQ-012 and WebTrust requirements and strictly controls its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the webCARES Digital Certificates issued by OATI during the period commencing immediately after the previous self-audit sample was taken."
9.6.1. CA Representations and Warranties	Compliant. CPS Section(s): 8.4	CPS Section 8.4 Other Warranties "Except as otherwise provided in Section 8.3 herein above and as provided in the CA/Browser Forum Baseline Requirements, OATI makes no other warranties of any kind."
9.6.3. Subscriber Representations and Warranties	Compliant. CPS Section(s): 8.1, 6.2, 6.3, 6.4; 3.3.1, 3.4.3, 3.4.6, 5.2,	CPS Section 8.1 Conditions of Usage of the webCARES Repository and Website "Any Subscriber or Relying Party accessing the webCARES official website(s) or repository shall abide by the provisions of this CPS and any other usage conditions made by webCARES and/or OATI. Parties confirm acceptance of the conditions of usage in the CPS by using an OATI webCARES issued OATI webCARES Digital Certificate. Failure to comply with the CPS conditions of usage of the webCARES repository and/or web site(s) may result in the termination of the relationship between OATI and the non-compliant party. This may result in immediate revocation of the non-compliant party's OATI webCARES Digital Certificate(s), and termination of

BR Section Number	Doc. & Sect. #	Explain how the CA's listed documents meet the requirements of each BR section.
		access to the OATI webCARES system. This CPS may be amended from time to time, and continued use of webCARES is an affirmation of acceptance of any such amendment(s)." CPS Section 6.2 Subscriber Obligations "OATI webCARES Subscribers shall be responsible for obligations as required by the CA/Browser Forum Baseline Requirements, v1.4.4 Section 9.6.3. which include but are not limited to the following: • To minimize internal risk of private key compromise. • To ensure the Public Key corresponds to the Private Key used. • To provide accurate and up to date information in its communications with webCARES. • To refrain from tampering with an OATI webCARES Digital Certificate. • To make reasonable efforts to prevent the modification, disclosure, compromise, loss, or unauthorized use of the Private Key. • To cease using an OATI webCARES Digital Certificate if any information is invalid, obsolete, or misleading. • To cease using an OATI webCARES Digital Certificate if the OATI webCARES Digital Certificate is expired or revoked. • To request a revocation for an OATI webCARES Digital Certificate in the occurrence the integrity of the OATI webCARES Digital Certificate is materially affected. • To cease using the OATI webCARES Digital Certificate if the Subscriber has no legitimate business purpose to use it. • To not share their personal OATI webCARES Digital Certificates. • To respond to OATI instructions regarding a compromise to the Private Key or misuse of the OATI webCARES Digital Certificate. CPS Section 6.3 Representations by Subscriber upon Acceptance "By accepting an OATI webCARES Digital Certificate, a Subscriber represents to OATI webCARES and other Relying Parties that at the time of acceptance and until further notice: • Subscriber has reviewed and verified the contents of the OATI webCARES Digital Certificate for accuracy. • Subscriber has installed the OATI webCARES Digital Certificate only on servers that are accessible at the subjectAltName(s) listed in the OATI webCARES Digital Certificate. • OATI webCARES Digital signatures created using the Private Key corresponding to the Public Key included in the OATI webCARES Digital Certificate is the Digital Signature of the Subscriber and the OATI webCARES Digital Certificate has been accepted and is properly operational at the time the Digital Signature is created. • No unauthorized person has ever had access to the Subscriber's private key. • All representations made by the Subscriber to webCARES regarding the information contained in the OATI webCARES Digital Certificate are accurate and true. • The OATI webCARES Digital Certificate is used consistent with this CPS and exclusively for authorized and legal purposes. CPS Section 6.4 Obligations of a Relying Party

BR Section Number	Doc. & Sect. #	Explain how the CA's listed documents meet the requirements of each BR section.
		To reasonably rely on the OATI webCARES Digital Certificate, a Relying Party must: • Trust an OATI webCARES Digital Certificate only if it is valid and has not been revoked or expired. • Verify the entire OATI webCARES Digital Certificate validation/trust chain to the issuing webCARES Root Certificate is intact and valid. • Minimize the risk of relying on an invalid, revoked, or expired OATI webCARES Digital Certificate by acquiring sufficient knowledge about using OATI webCARES Digital Certificates and signatures. • Read and agree with the terms of this CPS. • Verify the validity of the OATI webCARES Digital Certificate by referring to the relevant CRL." CPS Section 3.3.1 Security Officer/Local Registration Authority "The role of SO, otherwise known as a LRA, is mandatory for every organization or entity subscribing to the OATI webCARES system. A SO will be responsible for managing the Digital Certificates within his or her Organizational Unit. A SO will be responsible to use the OATI webCARES system to perform the SO's duties and responsibilities described in this CPS. A SO is delegated the right to serve as a LRA. The SOs duties and contractual obligations include, for example, issuing, revoking, renewing, and tracking OATI webCARES Digital Certificates for his or her End Users, and revoking OATI webCARES Digital Certificates for employees who leave the company. A SO will be provided personal access to the OATI webCARES system to perform his or her role. All SO webCARES users must follow CA Browser Baseline Requirements or risk revocation of Digital Certificate." CPS Section 3.4.3 OATI webCARES Digital Certificate Use "OATI webCARES Digital Certificates can be used for secure website access, in-house applications, internal client/device (mobile, Smart Grid, etc.) authentication, and encrypting and digitally signing email and documents. OATI webCARES Digital Certificates are not intended, and shall not be used for any transaction or data transfer that violates any applicable law or regulation. Any compromise or falsification of data or information provided to or in webCARES may result in prosecution, fines, or imprisonment." CPS Section 3.4.6 Conditions Requiring OATI webCARES Digital Certificate Revocation "Where the following conditions or circumstances occur, an OATI webCARES Digital Certificate issued by the OATI webCARES system must be immediately revoked. An SO is primarily responsible to revoke the OATI webCARES Digital Certificates with respect to any of the SO's users. Alternatively the OATI webCARES Administrator may also revoke the OATI webCARES Digital Certificate of an End Entity or SO: • When NAESB recommends that an ACA issued OATI webCARES Digital Certificate be revoked. • When the ACA reasonably suspects or becomes aware that the Private Key, or the media holding the Private Key, is suspected to be compromised or actually is compromised. • When the ACA becomes aware of an emergency which, if the OATI webCARES Digital Certificate is not revoked, may have material commercial impact to parties operation in accordance with the NAESB WEQ-012 Standards.

BR Section Number	Doc. & Sect. #	Explain how the CA's listed documents meet the requirements of each BR section.
		• When the SO or Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization. • When a Private Key, or the media holding the Private Key, is suspected to be compromised or actually is compromised. • When a party listed as the SO and/or BSO no longer represents a Business Organization. • When a device, server, or application is no longer active or no longer affiliated with the Subscriber's organization. • If the OATI CA learns, or reasonably suspects, that a Subscriber's Private Key has been compromised. • When a contract is terminated with OATI webCARES. • When requested, in writing, by an SO. • If a certificate is being used to promote malware or unwanted software OATI will revoke the certificate within a commercially-reasonable timeframe not to exceed two (2) business days from the date the request was received. • The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use. • The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g., a deprecated cryptographic/signature algorithm or key size might present an unacceptable risk and need to be revoked and replaced by CAs within a given period of time). OATI specifically reserves the right to revoke any OATI webCARES Digital Certificate issued by the OATI webCARES system for any issue relating to security or other national interest. Additionally, OATI reserves the right to provide federal, state and local agencies information relating to the application for, use of, and misconduct associated with any OATI webCARES Digital Certificate issued through the OATI webCARES system. In the event that the Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization, the SO would revoke the certificate." CPS Section 5.2 Private Key Protection "Subscribers are responsible for protecting the Private Key associated with the Public Key in the Subscriber's OATI webCARES Digital Certificate at all times. Subscribers must promptly notify OATI webCARES upon suspicion of loss or compromise of their private keys...
9.8. Limitations of liability	Compliant. CPS Section(s): 8.5, 10.1	CPS Section 8.5 Exclusion of Certain Elements of Damages "OATI specifically excludes liability for special damages, including but not limited to, indirect, punitive, or consequential damages arising out of the use, non-use, or inability to use webCARES, even if advised of the possibility of such damages." CPS Section 10.1 External Audits
9.9.1. Indemnification by CAs	Compliant. CPS Section(s): 8.8	CPS Section 8.8 Indemnification by CA "OATI shall defend, indemnify, and hold harmless an Application Software Supplier to the extent required by the CA/Browser Forum Baseline Requirements."
9.16.3. Severability	Compliant.	CPS Section 8.14 Severability

BR Section Number	*Doc. & Sect. #*	*Explain how the CA's listed documents meet the requirements of each BR section.*
	CPS Section(s): 8.14	“Any provision contained in this CPS that is held to be unenforceable shall not affect the other provisions in this CPS which shall be considered independent from the severable provision, and this CPS shall remain in full force and effect.”