BR Section Number	List the specific documents and section numbers of those documents which meet the requirements of each BR section	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.	DigiCert CP: Section 1.2 DOCUMENT NAME AND IDENTIFICATION DigiCert CPS: Section 1.2 DOCUMENT NAME AND IDENTIFICATION	DigiCert is fully compliant with the items listed in this table.
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.	DigiCert CP: Section 1.2 DOCUMENT NAME AND IDENTIFICATION DigiCert CPS: Section 1.2 DOCUMENT NAME AND IDENTIFICATION	DigiCert is fully compliant with the items listed in this table.
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.	DigiCert CPS: 1.3.2. Registration Authorities and Other Delegated Third Parties	This section of the DigiCert CPS indicates that DigiCert may delegate the performance of certain functions to third parties. Those parties are required to meet the requirements in section 5.3 for training and skills stated in the B.R..
2.1. Repositories Provide the direct URLs to the CA's repositories	DigiCert CP: Section 2.2 PUBLICATION OF CERTIFICATION INFORMATION DigiCert CPS: Section 2.1 REPOSITORIES	The CPS links directly to the following URL for the repository: http://www.digicert.com/legal-repository.htm
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)	DigiCert CPS: Section 1.1 OVERVIEW	"….This CPS describes the practices used to comply with the current versions of the following policies, guidelines, and requirements: the Certification Authority/Browser Forum (“CAB Forum”) Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”) located at https://cabforum.org/baseline-requirements-documents, □ the CAB Forum Guidelines for the Issuance and Management of Extended Validation Certificates (“EV Guidelines”) located at https://cabforum.org/extended-validation, □ the CAB Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates, □ the CAB Forum Network and Certificate System Security Requirements
2.2. Publication of information "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 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." --> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.	Digicert CPS: Section 2.2. PUBLICATION OF CERTIFICATION INFORMATION	For each root there are separate links listed beneath on this URL: https://www.digicert.com/digicert-root-certificates.htm

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.	Digicert CPS: Sections 1.1 OVERVIEW, and 9.12.1. Procedure for Amendment	CPS states:"This document specifies the policies DigiCert adopts to meet the current versions of the following policies, guidelines, and requirements: the Certification Authority / Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”) located at https://cabforum.org/baseline-requirements-documents," and "This CPS is reviewed annually. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the DCPA "
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.	Digicert CP: Sections 2.1 REPOSITORIES and 2.4. ACCESS CONTROLS ON REPOSITORIES	The CP states: "Issuer CAs shall publish all publicly trusted CA Certificates and cross-Certificates, issued to and from the Issuer CA, revocation data for issued digital Certificates, CP, CPS, and standard Relying Party Agreements and Subscriber Agreements in online repositories" and "Information published in a repository is public information. The Issuer CA shall provide unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories."
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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	Listed under the table for "IV and OV SSL/TLS Server, OSU Server, Object Signing, and Device Certificates (excluding device Certificates issued under the Grid-only arc)" the following statement is made to assert compliance with the CA/B Forum "DigiCert also verifies the identity and address of the Applicant using the procedures found in section 3.2.2.1 or section 3.2.3 of the Baseline 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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	Listed under the table for "IV and OV SSL/TLS Server, OSU Server, Object Signing, and Device Certificates (excluding device Certificates issued under the Grid-only arc)" the following statement is made to assert compliance with the CA/B Forum "DigiCert verifies any DBA included in a Certificate using a third party or government source, attestation letter, or reliable form of identification in accordance with section 3.2.2 of the Baseline Requirements "

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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	Listed under the table for "IV and OV SSL/TLS Server, OSU Server, Object Signing, and Device Certificates (excluding device Certificates issued under the Grid-only arc)" the following statement is made to assert compliance with the CA/B Forum "DigiCert validates the Applicant's right to use or control the Domain Name(s) and the country code that will be listed in the Certificate using the DV SSL/TLS Server Certificate validation procedures above." and "DigiCert verifies an included country code using (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; or (c) information provided by the Domain Name Registrar."
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 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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	Acceptable methods used are listed in the table of this section. The validation methodology is described below the table.
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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	The CPS states: "DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control....1. Validating the Applicant as a Domain Contact with the Domain Name Registrar provided that DigiCert has authenticated the Applicant's identity and the authority/agency of the Applicant Representative/Certificate Approver as required by the Baseline Requirements or EV Guidelines, respectively, performed in accordance with BR Section 3.2.2.4.1"
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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	The CPS states: "DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control....2. Email, Fax, SMS, or Postal Mail to the Domain Contact by sending a Random Value through email, fax, SMS, or postal mail, to the Domain Contact and receiving confirmation by their use of the Random Value, performed in accordance with BR Section 3.2.2.4.2;"

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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	The CPS states: "DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control....3. Phone call to the Domain Contact's phone number, as provided by the Domain Registrar, and receiving confirmation that the Applicant has requested validation of the Domain Name, performed in accordance with BR Section 3.2.2.4.3;"
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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	The CPS states: "DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control....4. Constructed Email to Domain Contact establishing the Applicant's control over the FQDN by sending an e-mail created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' as the local part followed by the ("@") sign, followed by an Authorization Domain name, including a Random Value in the e-mail, and receiving a response using the Random Value, performed in accordance with BR Section 3.2.2.4.4"
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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	The CPS states: "DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control....5. Relying upon a Domain Authorization Document that attests to the authority of the Applicant to request a Certificate for the Domain Name, provided that the Domain Authorization Document substantiates that it came from the Domain Contact and that (i) it is dated after the domain validation request or (ii) the WHOIS data has not materially changed since a previously provided Domain Authorization Document was provided, performed in accordance with BR Section 3.2.2.4.5"
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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	The CPS states: "DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control....6. An Agreed-Upon Change to the Website by the Applicant placing an agreed-upon Request Token or Request Value in the "/.well-known/pki-validation" directory, performed in accordance with BR Section 3.2.2.4.6;"

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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	The CPS states: "DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control....7. DNS Change by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character, performed in accordance BR Section 3.2.2.4.7;"
3.2.2.4.8 IP Address 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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	The CPS states: "DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control....8. IP Address - by confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Section 3.2.2.4.8;"
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.		The CPS states: "DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control....9. Test certificate issued by DigiCert on the Authorization Domain Name accessible by DigiCert over TLS at an Authorized Port, performed in accordance with BR Section 3.2.2.4.9;"
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.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	The CPS states: "DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control....10. TLS by confirming a Random Value within a Certificate on the Authorization Domain Name accessible by DigiCert over TLS at an Authorized Port, performed in accordance with BR Section 3.2.2.4.10."

3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, indicate how your CA meets the requirements in this section of the BRs.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	The CPS states: "DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control....8. IP Address - by confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Section 3.2.2.4.8;"
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 seciton of the BRs.	DigiCert CP: Section 3.2.2 Authentication of Organization and Domain Control	The CPS states: "If the FQDN contains a wildcard character, then the Issuer CA must remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation. Before issuing a certificate with a wildcard character in a CN or subjectAltName of a type DNS-ID, the CA must follow a documented procedure that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation). If a wildcard would fall within the label immediately to the left of a registry-controlled or public suffix, the Issuer CA must refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace."
3.2.2.7 Data Source Accuracy Indicate how your CA meets the requirements in this section of the BRs.	DigiCert CPS: Section 3.2.2 Authentication of Organization and Domain Control	The CP states: "If a publicly-trusted SSL/TLS Certificate will contain an organization's name, then the Issuer CA (or an RA) shall verify the information about the organization and its legal existence in accordance with Section 3.2.2.1 of the Baseline Requirements using reliable third party and government databases or through other direct means of communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition."
3.2.3. Authentication of Individual Identity	Digicert CPS: Section 3.2.3 Authentication of Individual Identity	Requirements in this section of the B.R. are met in the table described in this section, and subsequent subsections.
3.2.5. Validation of Authority	Digicert CPS: Section 3.2.5 Validation of Authority	Requirements in this section of the B.R. are met in the table described in this section, and subsequent subsections.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.		All cross certificates are listed here: https://www.digicert.com/digicert-root-certificates.htm

4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	Digicert CP: Section 4.1.1 Who Can Submit a Certificate Application Digicert CPS: Section 3.2.2 Authentication of Organization and Domain Identity	The CP states the following: "No individual or entity listed on a government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the United States may submit an application for a Certificate." The CPS states the following: "DigiCert maintains and utilizes a scoring system to flag certificate requests that potentially present a higher risk of fraud. Those certificate requests that are flagged “high risk” receive additional scrutiny or verification prior to issuance, which may include obtaining additional documentation from or additional communication with the Applicant."
4.1.2. Enrollment Process and Responsibilities	DigiCert CPS: Section 4.1.2 Enrollment Process and Responsibilities	The CPS states: "In no particular order, the enrollment process includes: □□ Submitting a certificate application, □□ Generating a Key Pair, □□ Delivering the Public Key of the Key Pair to DigiCert, □□ Agreeing to the applicable Subscriber Agreement, and □□ Paying any applicable fees. "
4.2. Certificate application processing		No description here in the B.R.
4.2.1. Performing Identification and Authentication Functions Indicate how your CA identifies high risk certificate requests.	DigiCert CPS: Section 4.2.1 Performing Identification and Authenticaation Functions	The CPS states: "If an RA assists in the verification, the RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to DigiCert. After verification is complete, DigiCert evaluates the corpus of information and decides whether or not to issue the Certificate. As part of this evaluation, DigiCert checks the Certificate against an internal database of previously revoked Certificates and rejected certificate requests to identify suspicious certificate requests. If some or all of the documentation used to support an application is in a language other than English, a DigiCert employee, RA, or agent skilled in the language performs the final cross-correlation and due diligence. "
4.2.2. Approval or Rejection of Certificate Applications	DigiCert CPS: Section 4.2.2 Approval or Rejection of Certificate Applications	The CPS states: "DigiCert rejects any certificate application that DigiCert or an RA cannot verify. DigiCert does not issue Certificates containing a new gTLD under consideration by ICANN until the gTLD has been approved."
4.3.1. CA Actions during Certificate Issuance	DigiCert CPS: Section 4.3.1 CA Actions during Certificate Issuance	The CPS states: "Certificate issuance by the Root CA requires an individual authorized by DigiCert (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation."
4.9.1.1 Reasons for Revoking a Subscriber Certificate Reasons for revoking certificates must be listed in the CA's CP/CPS.	DigiCert CPS: Section 4.9.1 Circumstances for Revocation	All revocation requirements in the B.R. are listed in this section.
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate	DigiCert CPS: Section 4.9.1 Circumstances for Revocation	All stated requirements for revoking a Subordinate CA are listed in this section of the DigiCert CPS.

4.9.2. Who Can Request Revocation	DigiCert CPS: Section 4.9.2 Who Can Request Revocation	The CPS states: "Any appropriately authorized party, such as a recognized representative of a subscriber or cross-signed partner, may request revocation of a Certificate. DigiCert may revoke a Certificate without receiving a request and without reason. Third parties may request certificate revocation for problems related to fraud, misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation."
4.9.3. Procedure for Revocation Request	DigiCert CPS: Section 4.9.3 Procedure for Revocation Request	This section of the DigiCert CPS provides instructions for applicants to request revocation of their own Certificates and it is continuously available 24/7. It also describes methods that can be used by Subscribers, Relying Parties, Application Software Suppliers, and other third parties that may need to report suspected key compromise, misuse, and other fraudulent uses of a certificate. The instructions are available through this CPS on a readily available legal repository, and on the DigiCert website.
4.9.5. Time within which CA Must Process the Revocation Request	DigiCert CP: Section 4.9.5. Time within which CA Must Process the Revocation Request	As stated in the CP: "The Issuer CA shall revoke other Certificates as quickly as practical after validating the revocation request. The Issuer CA shall process revocation requests as follows: 1. Before the next CRL is published, if the request is received two or more hours before regular periodic CRL issuance, 2. By publishing it in the CRL following the next CRL, if the request is received within two hours of the regularly scheduled next CRL issuance, and 3. Regardless, within 18 hours after receipt."
4.9.7. CRL Issuance Frequency	DigiCert CP: Section 4.9.7 CRL Issuance Frequency	The CP states, "For Issuer CAs and online intermediate CAs, the interval between CRL issuance shall not exceed 24 hours."
4.9.9. On-line Revocation/Status Checking Availability	DigiCert CPS Section 4.9.9 On-line Revocation/Status Checking Availability	The required formats in this section of the Baseline Requirements are stated in this section of the CPS. We perform both checks and meet both stated standards.
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 errounious return of "good" status.	DigiCert CPS section 4.9.10 On-line Revocation Checking Requirements	This section specifies how DigiCert supports OSCP capabilities using the GET method and does not respond with a "good" status for unissued or OCSP responder certificates.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	Digicert CPS: Section 4.9.11 Other Forms of Revocation Advertisements Available	This requirement is N/A and this section specifies no stipulation.
4.10.1. Operational Characteristics	Digicert CPS: Section 4.10.1 Operational Characteristics	The CPS states, "Certificate status information is available via CRL and OCSP responder. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period, except for revoked EV Code Signing Certificates, which remain on the CRL for at least 365 days following the Certificate's validity period. "

4.10.2. Service Availability	DigiCert CPS: Section 4.10.2 Service Availability	The CPS states: "Certificate status services are available 24x7 without interruption. This includes the online repository that application software can use to automatically check the current status of all unexpired Certificates issued by DigiCert. DigiCert operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions. DigiCert also maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint."
5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS		
5.2.2. Number of Individuals Required per Task	DigiCert CP: Sections 5.2.1.1 CA Administrators and 5.2.2 Number of Persons Required per Task	The CP states: "The CA Administrator is responsible for the installation and configuration of the CA software,including key generation, user and CA accounts, audit parameters, key backup, and key management.The CA Administrator is responsible for performing and securely storing regular system backups of the CA system. Administrators may not issue certificates to Subscribers" and "Each Issuer CA shall require that at least two people acting in a trusted role (one shall be a CA Administrator and the other cannot be an Internal Auditor) take action requiring a trusted role, such as activating the Issuer CA's Private Keys, generating a CA Key Pair, or creating a backup of a CA Private Key."
5.3.1. Qualifications, Experience, and Clearance Requirements	DigiCert CP: Section 5.3.1 Qualifications, Experience, and Clearance Requirements	The CP states: "The Issuer CA or the RA shall ensure that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CP."

5.3.3. Training Requirements and Procedures	Digicert CPS: Section 5.3.3. Training Requirements	The CPS states, "DigiCert provides skills training to all employees involved in DigiCert's PKI and TSA operations. The training relates to the person's job functions and covers: 1. basic Public Key Infrastructure (PKI) knowledge, 2. software versions used by DigiCert, 3. authentication and verification policies and procedures, 4. DigiCert security principles and mechanisms, 5. disaster recovery and business continuity procedures, 6. common threats to the validation process, including phishing and other social engineering tactics, and 7. CA/Browser Forum Guidelines and other applicable industry and government guidelines. Training is provided via a mentoring process involving senior members of the team to which the employee belongs.DigiCert maintains records of who received training and what level of training was completed. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All Registration Officers are required to pass an internal examination on the EV Guidelines and the Baseline Requirements prior to validating and approving the issuance of Certificates. Where competence is demonstrated in lieu of training, DigiCert maintains supporting documentation."
5.3.4. Retraining Frequency and Requirements	Digicert CP: Section 5.3.4. Retraining Frequency and Requirements	The CP states: "Personnel must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. The Issuer CA or RA shall make individuals acting in trusted roles aware of any changes to the Issuer CA's or RA's operations."
5.3.7. Independent Contractor Controls	DigiCert CP: Section 5.3.7 Independent Contractor Requirements	The CP states: "Any Issuer CA or RA allowing independent contractors to be assigned to perform trusted roles shall require that they agree to the obligations under this Section 5 (Facility, Management, and Operational Controls) and the sanctions stated above in Section 5.3.6. "
5.4.1. Types of Events Recorded	DigiCert CP: Section 5.4.1 Types of Events Recorded	The required items are listed in this section of the CP and CPS.
5.4.3. Retention Period for Audit Logs	DigiCert CPS: Section 5.5.2 Retention Period for Archive	The CPS states: "DigiCert retains archived data associated with Level 3 or Level 4, and federated device Certificates for at least 10.5 years. DigiCert, or the RA supporting issuance, archives data for other certificate types for at least 7.5 years."

5.4.8. Vulnerability Assessments	DigiCert CP: Section 5.4.8 Vulnerability Assessments	The CP states: "The Issuer CA shall perform routine risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. The Issuer CA shall also routinely assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the Issuer CA has in place to control such risks. The Issuer CA's auditors should review the security audit data checks for continuity and alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses."
5.5.2. Retention Period for Archive	DigiCert CPS: Section 5.5.2 Retention Period for Archive	The CPS states: "DigiCert retains archived data associated with Level 3 or Level 4, and federated device Certificates for at least 10.5 years. DigiCert, or the RA supporting issuance, archives data for other certificate types for at least 7.5 years."
5.7.1. Incident and Compromise Handling Procedures		
6.1.1. Key Pair Generation	DigiCert CP: Section 6.1.1. Key Pair Generation	The CP states the following: "Issuer CAs shall generate cryptographic keying material on a FIPS 140 level 3 validated cryptographic module using multiple individuals acting in trusted roles. When generating key material, the Issuer CA shall create auditable evidence to show that the Issuer CA enforced role separation and followed its key generation process. An independent third party shall validate that each CA key, including any root or intermediate CA keys associated with a Certificate cross-certified with the FBCA and each Root CA Key (for Certificates not cross-certified with the FBCA), is generated in accordance with this CP either by having the independent third party witness the key generation or by examining a signed and documented record of the key generation."
6.1.2. Private Key Delivery to Subscriber	DigiCert CP: Sections 6.1.2. Private Key Delivery to Subscriber and 4.9.1 Circumstances for Revocation	The CP states the following: "Except where escrow/backup services are provided, the key generator may not retain a copy of the Subscriber's Private Key after delivery…" and "If the Issuer CA, a CMS, or an RA generates keys on behalf of the Subscriber, then the entity generating the key shall deliver the Private Key securely (encrypted) to the Subscriber. The entity may deliver Private Keys to Subscribers electronically or on a hardware cryptographic module / SSCD." In section 4.9.1 it states, " The Issuer CA should revoke a Certificate if the Issuer CA is aware that:.... Either the Private Key associated with the Certificate or the Private Key used to sign the Certificate was compromised or misused;"

6.1.5. Key Sizes	DigiCert CP: Section 6.1.5. Key Sizes	All requirements specified by the CA/B Forum are met in this section. Due to length and inclusion of OCSP and CRL specifications, it is not posted within this response.
6.1.6. Public Key Parameters Generation and Quality Checking	DigiCert CPS: Section 6.1.6. Public Key Parameters Generation and Quality Checking	The CPS states: "DigiCert uses a cryptomodule that conforms to FIPS 186-2 and provides random number generation and on-board generation of up to 4096-bit RSA Public Keys and a wide range of ECC curves."
6.1.7. Key Usage Purposes	Digicert CPS: Section 6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)	The CPS states: "Private Keys corresponding to CA Certificates are not used to sign Certificates except in the following cases: 1. Self-signed Certificates to represent the Root CA itself; 2. Certificates for Subordinate CAs and Cross Certificates; 3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates; and 4. Certificates for OCSP Response verification"
6.2. Private Key Protection and Cryptographic Module Engineering Controls	DigiCert CPS: Section 6.2.1 Cryptographic Module Standardsa nd Controls	The CPS states: "DigiCert's cryptographic modules for all of its CA and OCSP responder Key Pairs are validated to the FIPS 140 Level 3 and International Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) 14169 EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) in the European Union (EU). IGTF Certificate Subscribers must protect their Private Keys in accordance with the applicable Guidelines on Private Key Protection, including the use of strong pass phrases to protect Private Keys. "
6.2.5. Private Key Archival	DigiCert CPS: Section 6.2.5. Private Key Archival	The CPS states, "DigiCert does not archive Private Keys."
6.2.6. Private Key Transfer into or from a Cryptographic Module	DigiCert CPS: Sections 6.2.6 Private Key Transfer into or from a Cryptographic M and 4.9.1 Circumstances for Revocation	The CPS states: "All keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, DigiCert encrypts the Private Key and protects the keys used for encryption from disclosure. Private Keys used to encrypt backups are securely stored and require two-person access If DigiCert becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinated CA, then DigiCert will revoke all certificates that include the Public Key corresponding to the communicated Private Key.." and "DigiCert may revoke any Certificate in its sole discretion, including if DigiCert believes that:...Either the Private Key associated with the Certificate or the Private Key used to sign the Certificate was compromised or misused."

6.2.7. Private Key Storage on Cryptographic Module	DigiCert CPS: Section 6.2.7 Private Key Storage on Cryptographic Module	The CPS states: " If the Issuing CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the Issuing CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key. "
6.3.2. Certificate Operational Periods and Key Pair Usage Periods	DigiCert CPS: Section 6.3.2 Certificate Operational Periods and Key Pair Usage Periods	The CPS specifies that the OV-SSL certificates abide by the requirements within the CA/B Forum and the EV SSL certificates have a certificate term of 825 days after 1 March 2018.
6.5.1. Specific Computer Security Technical Requirements	DigiCert CPS: Section 6.5.1 Specific Computer Security Technical Requirements	The CPS states: "DigiCert enforces multi-factor authentication on any account capable of directly causing Certificate issuance."
7.1. Certificate profile	Compliance to section 2.2: DigiCert CPS, Sections 1.1 Overview, 2.1 Respositories, 4.2.1 Performing Identification and Authentication Functions Compliance to section 6.1.5: DigiCert CP Section 6.1.5. Key Sizes Compliance to section 6.1.6: DigiCert CPS: Section 6.1.6. Public Key Parameters Generation and Quality Checking DigiCert CPS: Section 7 CERTIFICATE, CRL, AND OCSP PROFILES	Each of the listed sections complies with the technical requirements as listed in the previous entries. Section 7 of the CPS states: "DigiCert generates non-sequential Certificate serial numbers (positive numbers greater than zero) that contain at least 64 bits of output from a CSPRNG."
7.1.1. Version Number(s)	DigiCert CPS: Section 7.1.1 Version Number(s)	The CPS states: "All Certificates are X.509 version 3 Certificates."
7.1.2. Certificate Content and Extensions; Application of RFC 5280	This section specifies the additional requirements for Certificate content and extensions for Certificates generated after the Effective Date.	
7.1.2.1 Root CA Certificate	Profiles are published on the Legal Repository on DigiCert's website: https://www.digicert.com/wp-content/uploads/2018/01/Certificate-Profiles.pdf	The root CA certificate profile meets the stated requirements.
7.1.2.2 Subordinate CA Certificate	Profiles are published on the Legal Repository on DigiCert's website: https://www.digicert.com/wp-content/uploads/2018/01/Certificate-Profiles.pdf	The subordinate CA certificate profile meets the stated requirements.
7.1.2.3 Subscriber Certificate	Profiles are published on the Legal Repository on DigiCert's website: https://www.digicert.com/wp-content/uploads/2018/01/Certificate-Profiles.pdf	The subscriber CA certificate profile meets the stated requirements.
7.1.2.4 All Certificates	Profiles are published on the Legal Repository on DigiCert's website: https://www.digicert.com/wp-content/uploads/2018/01/Certificate-Profiles.pdf DigiCert CP: Section 7.1.2 Certificate Extensions	All certificate profiles meet the stated requirements. Also, the requirements are enforced in section 7.1.2 of the CP that states: "Issuer CAs shall use certificate extensions in accordance with applicable industry standards, including RFC 3280/5280. Issuer CAs shall not issue Certificates with a critical private extension. IGTF Certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125."

7.1.2.5 Application of RFC 5280	DigiCert CP: Section 7.1.2 Certificate Extensions	The CP states: "Issuer CAs shall use certificate extensions in accordance with applicable industry standards, including RFC 3280/5280. Issuer CAs shall not issue Certificates with a critical private extension. IGTF Certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125."
7.1.3. Algorithm Object Identifiers	DigiCert CPS: Section 7.1.3 Algorithm Object Identifiers	The CPS states: "SSL/TLS Server Certificates are not signed with sha-1WithRSAEncryption."
7.1.4. Name Forms	No requirement listed.	
7.1.4.1 Issuer Information	DigiCert CP: Section 7.1.4 Name Forms	The CP states: "The content of the Certificate Issuer Distinguished Name field must match the Subject DN of the Issuer CA to support name chaining as specified in RFC 5280, section 4.1.2.4."
7.1.4.2 Subject Information	Profiles are published on the Legal Repository on DigiCert's website: https://www.digicert.com/wp-content/uploads/2018/01/Certificate-Profiles.pdf	All certificate profiles meet the stated requirements.
7.1.4.3 Subject Information - Subordinate CA Certificates	The intermediate profiles and certificates are published here: https://www.digicert.com/digicert-root-certificates.htm#intermediates	All certificate profiles meet the stated requirements. To see the specifics, please go to: https://www.digicert.com/digicert-root-certificates.htm#intermediates
7.1.5. Name Constraints	DigiCert CPS: Sections 71.5 Name Constraints, 7.1.5.1. Name-Constrained serverAuth CAs, 7.1.5.2 Name-Constrained emailProtection CAs	Each section referenced in the CP meets the stated requirements in the CA/B Forum B.R..
7.1.6. Certificate Policy Object Identifier	No requirement listed.	
7.1.6.1 Reserved Certificate Policy Identifiers	Profiles are published on the Legal Repository on DigiCert's website: https://www.digicert.com/wp-content/uploads/2018/01/Certificate-Profiles.pdf Or Root and Intermediate certificates are posted here for review: https://www.digicert.com/digicert-root-certificates.htm	The Root CA, Subordinate CA, and Subscriber Certificate profiles include the appropriate policy identifiers to assert compliance to the CA/B Forum Baseline Requirements. Those that use 2.23.140.1.2.1 do not include organizationName, givenName, surname, streetAddress, localityName, stateOrProvinceName, or postalCode in the Subject field.
7.1.6.2 Root CA Certificates	Root and Intermediate certificates are posted here for review: https://www.digicert.com/digicert-root-certificates.htm	The Root CA certificate profile does not contain the certificatePolicies extension.
7.1.6.3 Subordinate CA Certificates	The intermediate profiles and certificates are published here: https://www.digicert.com/digicert-root-certificates.htm#intermediates DigiCert CPS: Section 1.2 DOCUMENT NAME AND IDENTIFICATION	The CPS states: "The specific OIDs used when objects are signed pursuant to this CPS are indicated in the object's respective Certificate Policies extension. For instance, when DigiCert issues a Certificate containing one of the above-specified policy identifiers for "Baseline Requirements," "Minimum Requirements," or "Extended Validation," it asserts that the Certificate was issued and is managed in accordance with those applicable requirements."

7.1.6.4 Subscriber Certificates	Profiles are published on the Legal Repository on DigiCert's website: URL GOES HERE DigiCert CPS: Section 1.1 Overview	End entity certs assert the 2.23.140.1.2.2 OID in the certificatePolicies. The CPS states the following to assert compliance to the B.R., "the Certification Authority/Browser Forum (“CAB Forum”) Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”) located at https://cabforum.org/baseline-requirements-documents"
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS		
8.1. Frequency or circumstances of assessment	DigiCert CPS: Section 8.1 Frequency or Circumstances of Assessment	The CPS states: "DigiCert receives an annual period in time audit by an independent external auditor to assess DigiCert's compliance with this CPS, referenced requirements, any applicable CPs, FPKIPA Audit Requirements, and the WebTrust for CA programs criteria. The audit covers DigiCert’s RA systems, Sub CAs, and OCSP Responders."
8.2. Identity/qualifications of assessor	DigiCert CPS: Section 8.2 Identity/Qualifications of Assessor	The CPS states: "WebTrust auditors must meet the requirements of Section 8.2 of the Baseline Requirements."
8.4. Topics covered by assessment	DigiCert CPS: Section 8.1 Frequency or Circumstances of Assessment	The CPS states: "DigiCert receives an annual audit by an independent external auditor to assess DigiCert's compliance with this CPS, referenced requirements, any applicable CPs, FPKIPA Audit Requirements, and the WebTrust for CA programs criteria. The audit covers DigiCert’s RA systems, Sub CAs, and OCSP Responders."
8.6. Communication of results	DigiCert CPS: Section 8.6 Communication of Results	The CPS states: "The results of each audit are reported to the DCPA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. Copies of DigiCert’s WebTrust for CAs audit reports can be found at: https://www.digicert.com/CPS. On an annual basis, DigiCert submits copies of its audit compliance reports to various parties, such as Mozilla, the Federal PKI Policy Authority, CA licensing bodies, etc."
8.7. Self-Audits	DigiCert CPS: Section 8.7 Self-Audits	The CPS states: "On at least a quarterly basis, DigiCert performs regular internal audits against a randomly selected sample of at least three percent of its SSL/TLS Server Certificates and EV Code Signing Certificates issued since the last internal audit. Self-audits on server and code signing Certificates are performed in accordance with Guidelines adopted by the CA / Browser Forum."
9.6.1. CA Representations and Warranties	DigiCert CPS: Section 9.6.1 CA Representations and Warranties	The CPS states, "Except as expressly stated in this CPS or in a separate agreement with a Subscriber, DigiCert does not make any representations regarding its products or services. DigiCert represents, to the extent specified in this CPS, that: DigiCert complies, in all material aspects, with the CP, this CPS, and all applicable laws and regulations..."
9.6.3. Subscriber Representations and Warranties	DigiCert CPS: Section 9.6.3 Subscriber Representations and Warranties	All listed requirements in the obligations and warranties of this section of the CA/B Forum are listed in this section of the CPS.

9.8. Limitations of liability	DigiCert CPS: Section 9.8 LIMITATIONS OF LIABILITY	DigiCert does assert compliance with the CA/B Forum Baseline Requirements in section 1.1 of the CPS, and this section does include the limitations of liability that are allowed in the B.R. as required.
9.9.1. Indemnification by CAs	DigiCert CPS: Section 9.9.1 Indemnification by DigiCert	The CPS states: "DigiCert shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by an Application Software Vendor related to an EV Certificate issued by DigiCert, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either (1) a valid and trustworthy EV Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) an EV Certificate that has expired or (ii) a revoked EV Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.
9.16.3. Severability	DigiCert CPS: Section 9.16.3 Severability	This section has no reference to a law due to no instances of conflict in the past. Should a conflict arise, DigiCert will handle it according to this CA/B Forum requirement.