

SYSTEM AND METHOD FOR VERIFIED COMPLIANCE IMPLEMENTATION**CROSS-REFERENCE TO RELATED APPLICATIONS**

[0001] This application claims the benefit of U.S. Patent Application No. 13/422,955, filed on March 16, 2012, and U.S. Patent Application No. 13/422,949, filed on March 16, 2012, which are incorporated herein by reference in their entirety for all purposes.

TECHNICAL FIELD

[0002] Embodiments of the present invention generally relate to systems and methods for automated compliance verification. More specifically, embodiments of the present invention relate to systems and methods for automatically verifying the accuracy of rules used in a compliance process.

BACKGROUND

[0003] Entities are often required to comply with rules set by various authorities on a wide variety of topics. For example, regulatory authorities may promulgate rules with respect to environmental protection or other compliance areas. Those rules may seek to control the amount of harmful substances that are produced, used, transported, or discarded by an entity. Overall, entities will need to conform to a potentially large number of rules on any number of issues, especially if those entities use remote sites located in satellite jurisdictions, which multiplies the number of rules with which those entities must comply. As part of their compliance efforts, many entities create compliance documents that identify rules pertinent to their operations. Those rules may change over time.

SUMMARY

[0004] To assist an entity in complying with, e.g., rules promulgated by regulatory authorities, some embodiments of the present invention operate to inform an entity of changes or updates to rules contained in its compliance documents. In particular, a compliance computer creates and sends a transmission object, which contains data referencing the rules contained in the compliance documents, to an operator server. The operator server searches for updates to the rules referenced in the transmission object and informs the entity if any updates are found. The transmission object may also reference jurisdictions and topics associated with the entity's operations, in which case the operator server uses that data to identify rules and/or updates to rules applicable to the entity's operations. The entity may then use the information from the operator server to update its compliance documents. In this manner, the entity accesses the most

current information and increases its ability to comply with all the pertinent rules in all relevant jurisdictions.

[0004a] According to a first aspect of the present invention, there is provided a computer-implemented method for a first entity to receive, from a second entity, an update to a compliance rule referenced in a compliance document of the first entity, the method comprising: analyzing the compliance document of the first entity using one or more processors in order to identify a reference to the compliance rule in the compliance document of the first entity and a section of the compliance document in which the compliance rule is referenced; creating metadata identifying the reference to the compliance rule and the section of the compliance document in which the compliance rule is referenced; creating a transmission object by the one or more processors by incorporating the metadata identifying the reference to the compliance rule and the section of the compliance document in which the compliance rule is referenced without incorporating the compliance document into the transmission object; sending the transmission object by the one or more processors to the second entity that uses the metadata identifying the reference to the compliance rule in the compliance document to identify an update to the compliance rule and that compiles the update to the compliance rule into a notification along with the metadata from the transmission object identifying the section of the compliance document in which the compliance rule is referenced; and receiving, from the second entity in response to the step of sending the transmission object, the notification identifying the update to the compliance rule and the section of the compliance rule in which the compliance rule is referenced.

[0004b] According to a second aspect of the present invention, there is provided a computer-based system for receiving updates to a compliance rule referenced in a company compliance manual while preserving privacy with respect to company-specific compliance policies in the compliance manual, the system comprising: one or more processors; an incorporation module configured to use the one or more processors to: parse a citation to a compliance rule in the company compliance manual from company-specific compliance policies regarding the compliance rule in the company compliance manual; and create a transmission object that includes the citation to the compliance rule in the company compliance manual without including the company-specific compliance policies regarding the compliance rule from the company compliance manual; a review module configured to use the one or more processors to present the

citation to the compliance rule in the transmission object to a user for approval; a communications module configured to send the transmission object to an entity responsible for receiving the transmission object, using the citation to identify updates to the compliance rule, and compiling the updates to the compliance rule into a notification; and an update module configured to use the one or more processors to receive the notification from the entity in response to sending the transmission object, the notification conveying an update to the compliance rule in the company compliance manual.

[0004c] As disclosed, there is provided a device comprising means for identifying a compliance rule in compliance documents pertinent to a satellite location of an entity; means for transmitting a portion of the compliance documents that includes the compliance rule to the satellite location, the portion of the compliance documents including a request for a set of information regarding whether the satellite location is adhering to the compliance rule; means for receiving the request at the satellite location; means, responsive to the request, for generating the set of information regarding whether the satellite location is adhering to the compliance rule; means for transmitting the set of information to the entity; and means for receiving the set of information at the entity.

[0004d] According to a third aspect of the present invention, there is provided a computer-implemented method for updating a compliance document with respect to regulatory changes without exposing potentially sensitive information in the compliance document, the method comprising: analyzing a compliance document of a first entity by one or more processors within a computer system of the first entity, wherein the compliance document includes a citation to at least one compliance rule at a specific location in the compliance document and at least one policy specific to the first entity regarding its compliance with the compliance rule, and wherein analyzing the compliance document includes: parsing the at least one policy specific to the first entity in the compliance document from the citation to the compliance rule in the compliance document; and identifying the specific location of the citation in the compliance document; creating a transmission object by the one or more processors within the computer system of the first entity by compiling the citation to the compliance rule from the compliance document and the specific location of the citation in the compliance document into the transmission object without including the at least one policy specific to the first entity from the compliance document; sending the transmission object by the one or more processors within the computer system of the first entity to an operator server of a second entity, wherein the operator server of the second

entity is configured to analyze the transmission object to extract the compliance rule in the transmission object, search an operator server database to identify an update to the compliance rule, analyze the transmission object to extract the specific location of the citation in the compliance document, and compile the update and the specific location of the citation in the compliance document into a notification; receiving the notification from the operator server of the second entity by the one or more processors within the computer system of the first entity in response to sending the transmission object to the operator server of the second entity, the notification including the update to the compliance rule from the operator server of the second entity and the specific location of the citation in the compliance document; and updating the compliance document of the first entity by the one or more processors within the computer system of the first entity using the update to the at least one compliance rule and the specific location of the citation in the notification from the operator server of the second entity.

[0005] While multiple embodiments are disclosed, still other embodiments of the present invention will become apparent to those skilled in the art from the following detailed description, which shows and describes illustrative embodiments of the invention. Accordingly, the drawings and detailed description are to be regarded as illustrative in nature and not restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Fig. 1 illustrates an exemplary networked environment in accordance with embodiments of the present invention and in which embodiments of the present invention may operate.

[0007] Fig. 2A illustrates an exemplary computer in accordance with embodiments of the present invention.

[0008] Fig. 2B illustrates an exemplary computer server in accordance with embodiments of the present invention.

[0009] Fig. 3 illustrates a flow chart depicting steps for completing a template and creating a transmission object according to embodiments of the present invention.

[0010] Fig. 4 illustrates software modules that may be used to perform some of the steps illustrated in the flow chart of Fig. 3.

[0011] Fig. 5 illustrates a flow chart depicting steps for receiving a transmission object and compiling and sending a notification reflecting a rule or a change to a rule using that transmission object according to embodiments of the present invention.

[0012] Fig. 6 illustrates software modules that may be used to perform some of the steps illustrated in the flow chart of Fig. 5.

[0013] Fig. 7 illustrates a flow chart depicting steps for transmitting updated compliance documents to satellite locations according to embodiments of the present invention.

[0014] Fig. 8 illustrates a flow chart depicting steps for completing and transmitting compliance documents according to embodiments of the present invention.

[0015] While the invention is amenable to various modifications and alternative forms, specific embodiments have been shown by way of example in the drawings and are described in detail below. The intention, however, is not to limit the invention to the particular embodiments described. On the contrary, the invention is intended to cover all modifications, equivalents, and alternatives falling within the scope of the invention as defined by the appended claims.

DETAILED DESCRIPTION

[0016] According to some embodiments of the present invention, an entity, for example a company operating coal-powered electric plants, creates compliance documents that assist the entity in complying with various rules pertinent to its operations, such as air pollution regulations. Because new rules may be added and existing rules altered or changed, for example, by the Environmental Protection Agency, the entity may wish to update its compliance documents by incorporating any regulatory updates pertinent to its operations into its compliance documents. At the same time, because compliance documents often contain sensitive or private information, the entity may not wish to transmit the compliance documents, and in particular the confidential information in the compliance documents, to unsecured or external sites.

[0017] To keep abreast of changes to pertinent rules, in some embodiments the entity creates and sends a transmission object to an operator server, which informs the operator server of rules referenced in the entity's compliance documents. At the same time, the transmission object may exclude confidential information found in the compliance documents. As used herein, the term "transmission object" refers to an object or other form of information that may be sent between two computers. A transmission object may be based on, for example, xml, html, or any other data format and may be used with any transmission protocol.

[0018] The operator server receives the transmission object and uses the data in the transmission object to identify updates to the rules referenced in the entity's compliance documents. In some embodiments, instead of referencing the rules contained in the compliance documents, or in addition to referencing those rules, the transmission object may contain data representing references to various jurisdictions in which the entity operates (e.g., New York) and/or topics relevant to the entity's operations (e.g., coal-powered electric plants or air pollution). The operator server receives that transmission object and searches for rules and updates to rules pertinent to those jurisdictions and/or topics. The operator server then communicates the identified updates or rules to the entity, which may then incorporate that information into its compliance documents.

[0019] Referring now to Fig. 1, several embodiments of the present invention (as well as environments in which they operate) utilize multiple computers connected over a network, such as the Internet. Specifically, a networked environment 100 may include an operator server 102 and an operator computer 104. The operator server 102 and the operator computer 104 are connected to a network 106, such as the Internet. The operator server 102 and/or the operator computer 104, either alone or in combination, receive transmission objects from various entities over the network 106 and use those transmission objects to identify rules or updates to rules

pertinent to each entity. For example, the operator server 102 receives a transmission object from an entity and reads that transmission object to identify rules referenced in that entity's compliance documents. The operator server 102 then searches a rules database (e.g., 264 in Fig. 2B), which contains updates to various rules in various jurisdictions, to identify specific updates to the rules in the transmission object. The operator server 102 then conveys those updates to the entity over the network 106. In some embodiments, the operator server 102 is also equipped to maintain one or more rules databases. In particular, and as explained in more detail below, the operator server 102 obtains and stores a variety of rules and updates to rules (e.g., modifications, interpretations, commentary, etc.) in one or more rules databases, for example, a remote data storage unit (264 in Fig. 2B).

[0020] Also connected to the network 106 is a compliance computer 108. The compliance computer 108 is typically located at an entity and is used to create and send the transmission object, and includes software (e.g., word processing programs) that enable a compliance implementer (e.g., a compliance officer) to draft and/or update compliance documents, such as a compliance manual. After the compliance computer 108 receives a notification from an operator server 102 that identifies changes to pertinent rules, the compliance computer 108 may be used to update the compliance documents.

[0021] One or more engineer (e.g., satellite) computers 110, 112, and 114 may be connected to the compliance computer 108 through a separate network 116. In some embodiments, the engineer computers 110, 112, and 114 are connected to the compliance computer 108 through the network 106. The networks 106 and 116 may be, e.g., the Internet, a local area network, a local intranet, or a cell phone network. The compliance computer 108 and/or the engineer computers 110, 112, and 114 may each be a smart phone, a tablet computer, a desktop computer, or any other computing device and, as explained below in more detail, may be used to audit or verify the entity's compliance with pertinent rules. For example, in some embodiments, once the compliance documents are updated, the compliance computer 108 sends those documents (or selected portions of those documents) to satellite locations to assist compliance personnel in completing audits or reports regarding each satellite location's compliance with the rules (and thus the entity's overall compliance with the rules). If those compliance documents include audit or reporting forms, the engineer computers 110, 112, and 114 are used to complete those forms and send the completed forms back to the compliance computer 108. The compliance computer 108 receives the completed audits or reports and compiles a final report that may be transmitted to internal or external authorities.

[0022] While Fig. 1 depicts a small networked environment, in some embodiments the networked environment 100 includes a plurality of operator servers 102, operator computers 104, networks 106, compliance computers 108, and/or engineer computers 110, 112, or 114.

[0023] Fig. 2A illustrates a computer system 200, and aspects thereof, that may serve as an operator computer 104, a compliance computer 108, and/or an engineer computer 110, 112, or 116. The illustrated computer system 200 includes a processor 204 coupled to a memory 206 and a network interface 208 through a bus 210. The network interface 208 is also coupled to a network 212 such as the Internet. The computer system 200 may further include a monitor 214, a keyboard 216, and a mouse 218. In other embodiments, the computer system 200 may use other mechanisms for data input/output and may include a plurality of components (e.g., a plurality of memories 206 or buses 210). Fig. 2B illustrates a computer server 250 and aspects thereof, which may serve as an operator server 102. The illustrated computer server 250 includes a processor 254 coupled to a memory 256 and a network interface 258 through a bus 260. The network interface 258 is also coupled to a network 262 such as the Internet. In other embodiments, the computer server 250 may include a plurality of components (e.g., a plurality of memories 256 or buses 260). The network 262 may include a remote data storage system including a plurality of remote storage units 264 configured to store data at remote locations. Each remote storage unit 264 may be network addressable storage. In some embodiments, the computer system 200 and/or the computer server 250 include a computer-readable medium containing instructions that cause the processor 254 to perform specific functions that will be described in more detail below. That medium may include a hard drive, a disk, memory, or a transmission, among other computer-readable media.

[0024] The flow chart shown in Fig. 3 illustrates specific steps that the compliance computer 108 (automatically and/or in conjunction with the compliance officer) may perform. Not every step shown in Fig. 3 is used in every embodiment, and different embodiments include various combinations of the steps shown in Fig. 3 or possibly additional steps than those shown in Fig 3.

[0025] In some embodiments, before creating the transmission object or perhaps even before creating the compliance documents, the compliance computer 108 (automatically and/or in conjunction with the compliance officer) creates a profile as shown in block 302. The profile contains information about the entity, such as, for example, jurisdictions in which it operates, general areas of operation, specific rules or areas of regulation with which the entity may be concerned, the frequency at which the entity wishes to receive updates, an identifier for that entity, and/or other information related to the entity and its operations. The compliance computer 108 may automatically create select portions of the profile or it may automatically

create all of the profile. If the compliance officer is involved in creating the profile (in whole or in part), the compliance computer 108 may access a set of questions that are stored, e.g., on the operator server 102 to assist the compliance officer in completing the profile. The completed profile is then transmitted to the operator server 102, which uses a profile receiver to receive the profile. The operator server 102 then stores the completed profile in its memory.

[0026] As shown in block 304, the compliance computer 108 is also used to create initial compliance documents. In some embodiments, the profile (in particular the information contained in the profile) is used to assist in the creation of the initial compliance documents. Specifically, the operator server 102 uses the profile to identify and transmit specific information to the operator computer 108 to guide the compliance officer in drafting the initial compliance documents. For example, if the profile indicates that the entity is involved in coal-powered electric plants, the operator server 102 may create and transmit a custom document or transmission that prompts the compliance officer to input particular information into specific sections of the initial compliance documents (e.g., a prompt suggesting that key terms or phrases associated with carbon dioxide or coal-powered electric plants be placed into section 7(d) of the initial compliance documents). In some embodiments, the compliance computer 108 automatically incorporates the information sent by the operator server 102 into the initial compliance documents, e.g., into the specific sections identified by the operator server 102. The profile may also be used when creating and/or completing a template, as discussed below in more detail.

[0027] The initial compliance documents may include, for example, a compliance manual, audit forms, audit instructions, reporting forms, and/or reporting instructions. The initial compliance documents may also include pictures, illustrations, measurements, diagrams, charts, etc. In general, the initial compliance documents include information relating to the rules with which the entity (e.g., a company) must comply. A rule may be a law, regulation, recommendation, standard, guideline, and/or provision intended to direct, control, and/or monitor a company's actions, whether formally or informally. Some rules are external rules promulgated by regulatory authorities that operate on a local, regional, national, and/or international level. Other rules may be internal rules issued by the company itself. For example, if a particular state regulation limits the amount of carbon dioxide emissions to 1,100 lbs. per megawatt-hour, the company may issue an internal rule that requires less than 1,000 lbs. per megawatt-hour. The rules may apply to any number of topics, such as manufacturing, retail, transportation, health, medical equipment, pharmaceuticals, food, education, workplace safety, privacy, communications, labor/employment, financial, billing, human resources, cross-border

finances, etc. For example, the Foreign Corrupt Practices Act and Anti-Money Laundering Laws are designed to target international and cross-border actions.

[0028] In some embodiments, the initial compliance documents indicate one or more jurisdictions (e.g., Ohio, China) in which the company operates. The initial compliance documents may also indicate a topic (e.g., air pollution) or a specific rule (e.g., a regulation issued by the Environmental Protection Agency or a particular guideline or standard internal to the company). Thus, the initial compliance documents may include references to specific rules, references to topics pertinent to the entity's operations, references to the jurisdictions in which the entity is operating, and/or other, similar information. In addition, the initial compliance documents may designate specific steps and procedures for identifying and reporting a company's compliance with those rules and standards. For example, in some embodiments, the initial compliance documents identify particular evidence (e.g., photographs) that should be submitted during an audit.

[0029] The initial compliance documents may also instruct users on how to respond if the company is not in compliance with one or more rules. For example, the initial compliance documents may direct employees to inform specific compliance agencies or individuals within the company of a failure to comply. Thus, the initial compliance documents may include confidential information about how the entity plans to act with respect to one or more rules, guidelines for ensuring compliance, or actions to take if the entity is not in compliance with one or more rules, or other information of a confidential nature. Other examples of confidential information include employee identification (names, positions, etc.), internal standards that differ between satellite locations, statements that the entity emits certain substances (e.g., carcinogenic substances) even if the amounts emitted are below the standards set in the rules, etc.

[0030] According to some embodiments, after the initial compliance documents are complete, the compliance computer 108 receives a template, as shown in block 306. The template may be generated by the operator server 102 using a template generator. The template can be a computer object based on, for example, xml code or javascript. The template may use any coding formats compatible with, for example, word processing documents, html, xml, etc. In some embodiments, the template contains instructions or prompts that assist the compliance officer and/or compliance computer in completing the template. Those instructions or prompts may be generated using the information in the entity's profile. In other embodiments, the template does not contain instructions or prompts of any kind.

[0031] The template is used to store tags or metadata identifying the rules in the initial compliance documents or the jurisdictions and/or topics relevant to the entity's operations. The

compliance computer 108 (possibly in conjunction with the compliance officer) completes the template using the compliance documents, as shown in block 308. In some embodiments, to complete the template, the compliance computer 108 (possibly in conjunction with the compliance officer) first creates metadata or tags to identify the jurisdictions, topics, and/or specific rules referenced in the initial compliance documents. The metadata or tags may also identify the specific sections of the initial compliance documents, for example, page 4 or section 2(b), where the jurisdictions, topics, and/or specific rules are referenced. The compliance computer 108 (possibly in conjunction with the compliance officer) then completes the template by incorporating those tags or metadata into the template.

[0032] In some embodiments, the compliance computer 108 includes software that enables it to automatically search the initial compliance documents for references to jurisdictions, topics, rules, or similar information, and automatically compile that information into the template. For example, Fig. 4 illustrates various software modules 400 that the compliance computer 108 may execute as part of that process. Those software modules 400 may be written in programming languages such as, for example, C#.NET or Java. The software modules 400 may communicate with each other in any number of ways. For example, when the compliance computer 108 executes the compliance document search module 402, it creates data that is accessed when the compliance computer 108 executes the compliance document tagging module 404. The other software modules may likewise communicate with each other.

[0033] In particular, in some embodiments, the compliance document search module 402 operates to search the initial compliance documents for key terms or phrases, for example, using a text-based search that matches the content of the initial compliance documents against a pre-formed list of key terms or phrases. In some embodiments, the set of key terms or phrases used by the search module 402 include key terms or phrases associated with jurisdictions (e.g., Ohio, China, etc.) and/or topics (e.g., Air Pollution, CO₂, Power Plants, etc.), among other information, which can be used to identify one or more rules. The set of key terms and phrases may also include key terms or phrases that directly identify one or more rules (e.g., CFR). The set of key terms or phrases may be customized for a particular entity. For example, if the entity operates coal-powered electric plants, the compliance document search module 402 may be programmed to search the compliance documents for particular key terms (e.g., carbon dioxide, parts per million, scrubbing, etc.) or particular regulations (e.g., specific EPA regulations). In some embodiments, the set of key terms or phrases is compiled based on information in the entity's profile. For example, if the entity's profile identifies particular jurisdictions (e.g., New York) or industries (e.g., coal-powered electric plants), the set of key terms or phrases would include key terms or phrases specific to those jurisdictions and/or industries. If the initial

compliance documents were drafted with key terms or phrases in specific sections of the compliance documents, then the compliance document search module 402 may search only those particular sections for the key terms or phrases. The set of key terms or phrases may be sent from the operator server 102 to the compliance computer 108 (and in particular the compliance document search module 402).

[0034] Once the compliance document search module 402 identifies one or more key terms or phrases in the initial compliance documents, the compliance document tagging module 404 operates to create tags or metadata identifying the rules, jurisdictions, topics, and/or key terms or phrases in the initial compliance documents. The compliance document tagging module 404 may also create tags or metadata identifying the section or sections of the initial compliance documents that reference the rules, jurisdictions, topics, and/or key terms or phrases. An incorporation module 406 then operates to compile the tags or metadata into a separate computer object. That computer object may be the template or it may be a transmission object, which is discussed in more detail below. In some embodiments, after the incorporation module 406 has compiled the tags or metadata, a review module 408 presents the tags or metadata to the compliance officer. The compliance officer then reviews and approves the tags or metadata. In addition, the compliance officer may use the review module 408 to add new tags or metadata, edit the existing tags or metadata, or remove tags or metadata.

[0035] According to some embodiments, the completed template includes only the tags or metadata associated with the initial compliance documents, without including specific language, particular policies, or other confidential information contained in the initial compliance documents. For example, the initial compliance documents may reference multiple jurisdictions (e.g., New York, Ohio, and China), a topic (e.g., air pollution), and multiple rules (e.g., specific regulations by the EPA) associated with its operations in particular sections of the compliance documents (e.g., rules relating to air pollution in New York may be in section 7(d) of the initial compliance documents and rules relating to air pollution in Ohio may be in section 12(b) of the initial compliance documents). The compliance documents may further include confidential information, such as actions to take if the entity is not in compliance. The compliance computer 108, perhaps in conjunction with the compliance implementer, searches the initial compliance documents and creates tags that identify the jurisdictions, the topic, the rules, as well as the sections in which they are referenced. Only those tags or metadata are placed into the template, such that the confidential information remains solely in the initial compliance documents.

[0036] Referring back to step 304 and 306 of Fig. 3, in some embodiments the template is received (step 306) before the initial compliance documents are created (step 304). In those

embodiments, the template may include specific information to assist the compliance officer and/or compliance computer 108 in creating the initial compliance documents. For example, if the profile indicates that the entity is involved in coal-powered electric plants, the operator server 102 may create and transmit a custom template that directs the compliance officer and/or compliance computer 108 to input particular information into specific sections of the template. In particular, the template may prompt the compliance officer to input key terms associated with carbon dioxide or coal-powered electric plants into section 7(d) of the template. The template may also prompt the compliance officer to input specific information into the template, such as how old the coal-powered electric plants are. In other words, these prompts may assist the compliance officer in identifying and supplying key terms relevant to the pertinent rules, or the prompts may be more general questions designed to guide the compliance officer in a more general fashion. In the embodiments in which the template prompts the compliance officer to input information into the template itself, the completed template may operate (in whole or in part) as the initial compliance documents. In those embodiments, the software modules 400 shown in Fig. 4 may be modified to operate on the template, rather than on the initial compliance documents themselves.

[0037] As shown in block 310 in Fig. 3, the compliance computer 108 uses the metadata or tags in the template to create a transmission object. Alternatively (or in addition), the compliance computer 108 may compile that tags or metadata directly into the transmission object. In some embodiments, the compliance computer 108 uses the incorporation module (406 in Fig. 4) to incorporate the tags or metadata created by the compliance document tagging module 404 into the transmission object. The incorporation module 406 may include only the tags or metadata from the compliance document tagging module 404, such that the transmission object will not include confidential information, for example, regarding how the entity intends to comply with the rules. The transmission object may also include specific search requests (e.g., articles in the New York Times discussing coal-powered electric plants in the last six months) for the operator server 102 to perform.

[0038] Once created, the transmission object is sent to the operator server 102, as shown in block 312 of Fig. 3. The transmission object may be sent wirelessly using a cellular telephone connector, wireless internet adaptor, through a wired connection to the Internet, or using any other communication structure.

[0039] In some embodiments, the operator server 102 is specifically programmed to perform certain functions, some of which are illustrated in Fig. 5. Not every step shown in Fig. 5 is used in every embodiment, and different embodiments include various combinations of the steps (or possibly additional steps than those) shown in Fig. 5. In addition, Fig. 6 illustrates

software modules 600 that the operator server 102 may execute when performing one or more of the steps listed in Fig. 5. Like the software modules 400, the software modules 600 may communicate with each other in a variety of ways.

[0040] In some embodiments, the operator server 102 maintains one or more rules databases (using, e.g., the remote storage units 264 in Fig. 2B) that contain data regarding rules and updates to rules. In particular, the operator server 102 maintains the rules databases in order to monitor any changes to any rules by, e.g., the pertinent regulating agency. The operator server 102 may also monitor sources interpreting rules (e.g., judicial decisions), as well as the issuance of subsequent rules (e.g., regulations or statutes) that modify, repeal, or otherwise affect an existing rule or its implementation. The operator server 102 may also be configured to monitor secondary sources, such as news articles, law review articles, blog commentary, etc., that reference one or more rules. Thus, an update to a rule may include specific changes to the rule as well as commentary on the rule or its implementation. In some embodiments, the operator server 102 compiles and/or maintains the rules databases before receiving any profiles or transmission objects. In those embodiments, the rules databases include rules that may not be referenced in any particular transmission object. In other embodiments, the operator server 102 compiles and/or maintains the rules databases based on information contained in profiles or in transmission objects.

[0041] The operator server 102 may automatically maintain those rules databases (and monitor the sources mentioned above) in a variety of fashions. For example, referring to Fig. 6, the operator server 102 may execute an update search module 602 that actively searches for updates to rules. For example, the update search module 602 may be configured to search a specific database (e.g., an external database of a regulating agency) to which updates to rules are published in order to identify rules that have been issued or modified by that regulating agency. The update search module 602 may also search databases that compile and publish rules updates to rules in many jurisdictions relating to many different topics. In some embodiments, the update search module 602 searches for specific key terms identified in a predetermined list of key terms, and/or may search for terms that identify a particular source of rules (e.g., “CFR”). In addition to those sources, the update search module 602 may searching the Internet for news stories or blog commentary referencing rules. The update search module 602 may also receive messages that inform the operator server 102 that one or more rules have been modified or amended.

[0042] For example, if the Ohio EPA changed the standards set in OAC 3745-19, the operator server 102 may receive the changes to OAC 3745-19 through a received message and/or through active searching by the update search module 602. The operator server 102

stores that information in the rules databases (e.g., remote database 264 in Fig. 2B). In particular, the operator server 102 may store data indicating that OAC 3745-19 was amended, the date that OAC 3745-19 was amended, and/or the specific changes made to that rule. Again, references to OAC 3745-19 are exemplary only; each notification may relate to a variety of rules in any number of jurisdictions, federal or state, national or international. In addition, each message may simply indicate that a rule was referenced in a secondary source or may include a copy of that secondary source.

[0043] When compiling data into the rules databases, the operator server 102 may use a database tag module (604 in Fig. 6) that automatically associates sets of data (e.g., rules or updates to rules) with particular key terms, tags, or metadata. For example, if a rules database includes a news article discussing the potential effects of a proposed change to one of Ohio's "Open Burning Standards," the database tag module 604 tags that news article with metadata referencing the specific rule discussed in the article, as well as general terms identifying the topic (e.g., Air Pollution) and/or jurisdiction (Ohio). In some embodiments, an operator uses the operator server 102 or operator computer 104 to manually add metadata or tags to the data in the rules databases alone or in conjunction with the database tag module 604.

[0044] Referring now to Fig. 5, the operator server 102 receives a transmission object from a compliance computer 108, as shown in step 502. The operator server 102 may receive multiple transmission objects from different compliance computers 108. The operator server 102 may receive the transmission objects using a wireless connection, such as a cell phone or a wireless internet adaptor, or may receive the transmission object over a wired connection to, e.g., the Internet. The operator server 102 stores the transmission objects in memory, as shown in block 504. The memory may be a local memory or may be a remote storage unit 264 in Fig. 2B. The operator server 102 may sort and organize each transmission object by the compliance computer 108 and/or compliance officer that sent the transmission object. The sorting and organizing step may include adding additional metadata or tags to each transmission object that reference, for example, identification information provided in the profile of each entity.

[0045] The operator server 102 reads the data in each transmission object and identifies one or more rules (e.g., OAC 3745-19, which is a regulation promulgated by the Ohio Environmental Protection Agency relating to "Open Burning Standards") associated with each transmission object, as shown in block 506. The operator server 102 may then search the rules databases for updates to those identified rules, as shown in block 508. If the transmission object does not directly identify a rule, for example, if the transmission object identifies only a jurisdiction and/or topic, the operator server 102 searches the rules databases for applicable (and, in some embodiments, updated) rules pertinent to the jurisdiction and/or topic. To search the

rules databases for pertinent updated rules and/or updates to identified rules, the operator server 102 may use a compare module (606 in Fig. 6) that extracts the information (e.g., metadata or tags) in each transmission object and compares that information to the data (e.g., the metadata or tags created by the database tag module 604) in the rules databases. The compare module 606 may use a search algorithm to match key terms, or may use a different set of criteria to identify changes to the rules referenced in each transmission object. Thus, the operator server 102 may use the rules databases to generate a set of information that identifies the most accurate rules pertinent to the entity and its operations.

[0046] The operator server 102 uses that set of information to create or compile a notification, as shown in block 510 in Fig. 5. In particular, the operator server 102 may use a notification compilation module (608 in Fig. 6), which receives information from the compare module 606 and incorporates that information into a notification. The notification is a computer object that may be based on, for example, xml, html, or any other data format. In some embodiments, the notification compilation module 608 incorporates into the notification the specific section or sections of the template or initial compliance documents (e.g., page 4 or section 2(b)) in which the rule (e.g., OAC 3745-19) is referenced, using data from the transmission object. If a rule has been modified, the notification may contain the specific changes to the rule or may simply indicate that the rule was changed. If the rule has been referenced in a secondary source, the notification may include a copy of that secondary source or may simply provide reference information for that secondary source.

[0047] For a specific example, the operator server 102 receives a message indicating that OAC 3745-19 was amended or, using the update search module 602, may discover that OAC 3745-19 was amended. The operator server 102 then stores, in the rules databases, data indicating that OAC 3745-19 was amended, the date OAC 3745-19 was amended, the specific changes to OAC 3745-19, and/or other information pertinent to that rule and the changes to that rule. The operator server 102 then uses the database tag module 604 to add metadata identifying the rule itself, the jurisdiction (Ohio), the topic (Air Pollution) and/or other metadata relevant to that rule (e.g., other key terms such as CO₂). The operator server 102 uses the compare module 606 to search each stored transmission object and extract the metadata or tags therein, and then compares the metadata in the transmission object to the metadata created by the tag module 604. If the metadata stored in the transmission object includes, e.g., a reference to OAC 3745-19, Ohio, and/or air pollution (or other key terms), the compare module 606 sends data regarding the updated rule (and its associated metadata) to the notification compilation module 608, which creates a notification that incorporates the information received from the compare module 606.

[0048] As shown in block 512 of Fig. 5, the operator server 102 sends the notification to the compliance computer 108 that sent the transmission object. The operator server 102 may send that notification wirelessly, using a cellular telephone connector or a wireless internet adaptor, or it may send the notification over a wired connection (e.g., a modem) through the Internet. That process may be repeated for each transmission object. In some embodiments, the operator server 102 is configured to send a notification to each compliance computer 108 on a regular basis to report any changes in the jurisdictions, the topics, and/or the rules identified in the templates. In other embodiments, the operator server 102 is configured to transmit notifications whenever a change in the rules is detected or whenever the compliance computer 108 requests a notification.

[0049] Once the compliance computer 108 receives the notification from the operator server 102, the compliance computer 108 (possibly in conjunction with the compliance officer) updates the initial compliance documents using the information in the notification. For example, in embodiments in which the notification identifies the section or sections in the initial compliance documents that reference the rule or rules in the notification, the compliance officer can quickly move to those sections and incorporate the updates. In some embodiments, the operator computer 108 may update the compliance documents automatically using a compliance document update module (410 in Fig. 4). For example, the compliance document update module 410 searches the received notification and identifies OAC 3745-19 as a modified rule. The compliance document update module 410 searches the compliance documents for the appropriate place to update the compliance documents. If the notification includes a reference to the section or sections in the initial compliance documents that reference the modified rules, the compliance document update module 410 may use that information to quickly and accurately update the compliance documents.

[0050] More specifically, in the course of updating the compliance documents, the compliance document update module 410 may use the metadata referencing the section or sections of the initial compliance document in which a rule (e.g., OAC 3745-19) was referenced, or it may search the initial compliance documents for direct references to that rule. The compliance document update module 410 may also search the metadata created by the compliance document tagging module 404 for terms related to OAC 3745-19. Once the appropriate location or locations are identified, the compliance document update module 410 incorporates the changes for OAC 3745-19 into the compliance documents. That step may involve substituting the entire text of OAC 3745-19, adding the text of amended OAC 3745-19 next to the original OAC 3745-19, adding or substituting only the amended sections of OAC

3745-19, or simply adding a reference to where a compliance implementer may access OAC 3745-19 as amended.

[0051] In some embodiments, the compliance document update module 410 propagates the changes made to in a particular section of the compliance documents to other sections of the compliance documents. For example, the compliance officer (and/or compliance computer 108) may use the notification to update a rule in a particular section of the compliance manual. The compliance computer 108 may then make similar changes to related sections of, for example, auditing documents that use the rules and procedures as set by the compliance manual.

[0052] According to some embodiments, the compliance computer 108 is configured to transmit the updated compliance documents to one or more engineer computers (e.g., engineer computer 110, 112, and/or 114), receive compliance information from those engineer computers, and compile a report. Fig. 7 illustrates exemplary steps that may be used by the compliance computer 108 when interfacing with the engineer computers, though not every step shown in Fig. 7 is used in every embodiment and different embodiments include various combinations of the steps (or possibly additional steps than those) shown in Fig. 7. In those embodiments, the compliance computer 108 identifies one or more satellite locations, as shown in step 702. In some embodiments, this can be done using a satellite identification module (412 in Fig. 4). Referring back to Fig. 4 (with some reference to Fig. 7), the satellite identification module 412 operates by sorting through a locally-stored list of satellite locations on the compliance computer 108. The satellite identification module 412 transmits that data to a satellite compliance module 414. The satellite compliance module 414 transmits the updated compliance documents to the satellite location (e.g., to the engineer computers at each satellite location) using, for example, a cellular telephone connector or wireless internet adapter. The satellite compliance module 414 may also transmit the updated compliance documents using a wired connection, for example, a modem connection to the Internet. This transmission is also indicated by step 704 of Fig. 7.

[0053] In some embodiments, the satellite compliance module 414 does not transmit all of the compliance documents, but instead identifies and transmits only those documents or portions of documents pertinent to each satellite location. For example, if the satellite identification module 412 identifies a satellite office in Ohio, the satellite compliance module 414 could extract the compliance documents or portions of the compliance documents pertinent to Ohio (e.g., those documents referencing OAC 3745-19). Other documents identified and transmitted by the satellite compliance module 414 may include a request for information in the form of an audit and/or reporting form (along with instructions on how to complete each form) for engineers and/or compliance personnel at each satellite location. To identify the pertinent compliance documents or the pertinent portions of the compliance documents, the satellite

compliance module 414 may use (in whole or in part) the tags and/or metadata created by the compliance document tagging module 404. Other information that may be used by the satellite compliance module 414 (and gathered by the satellite compliance module 414 from, e.g., an internal database) may include the experience and/or responsibilities of the compliance personnel at each satellite location.

[0054] The auditing and reporting forms are completed by engineers and/or compliance personnel at each satellite location, as described in more detail below. The engineers and/or compliance personnel transmit the information required by the audit or reporting forms to the compliance computer 108. As shown in step 706, the compliance computer 108, and, e.g., the satellite compliance module 414 in particular, may receive that compliance information over the Internet or over a secured connection using, e.g., a cellular telephone connector, a wireless internet adapter, or a wired connection such as a modem. Thus, the compliance computer 108 may communicate with the engineer computers 110, 112, and/or 114 via the Internet or through a private network. In some embodiments, the compliance computer 108 may be configured to transmit the compliance documents on a regular basis (e.g., monthly or quarterly) or may be configured to transmit the compliance documents upon instruction.

[0055] In some embodiments, the satellite compliance module 414 automatically compares the information transmitted from each satellite location to the standards set in the updated compliance documents. In other embodiments, the satellite compliance module 414 assists the compliance implementer in comparing the data transmitted from the satellite locations to the standards in the updated compliance documents. Whether operating to automatically compare the data or assisting the compliance implementer in comparing the data, the satellite compliance module 414 may use the tags and/or metadata in the updated compliance documents to quickly identify relevant sections of the updated compliance documents and/or the information contained therein.

[0056] By comparing the data received from the satellite locations to the rules in the updated compliance documents, the compliance computer 108 (automatically and/or in conjunction with the compliance officer) may verify the compliance of each satellite office with the pertinent rules. A report may then be compiled, as shown in step 708 of Fig. 7, which details the compliance of one or all of the satellite locations with their respective rules. In particular, the compliance computer 108 may use a report module 416, which collects compliance data (e.g., statistics, raw data transmitted from the satellite locations, etc.) from the satellite compliance module 414 and creates a report using that data.

[0057] In some embodiments, the report module 416 reformats the data received from the engineer computers into a format required by the regulatory authorities. For example, the

updated compliance documents may ask for data in a format convenient for the engineer and/or compliance personnel (e.g., the amount of carbon dioxide in cubic meters) while the pertinent rules may require that the data be submitted to authorities by weight rather than volume. In other scenarios, the updated compliance documents may ask for data in a proprietary format (e.g., by referencing the number or size of products produced). In those embodiments, the report module 416 automatically converts the data into a format compatible with pertinent rules. Once the reports are compiled, the compliance computer 108 (automatically and/or in conjunction with the compliance officer) may transmit those reports to the pertinent authorities (whether external regulators or internal auditors).

[0058] Fig. 8 illustrates steps that may be performed (in whole or in part) by the engineer computers 110, 112, 114 to submit compliance data to the compliance computer 108. Not every step shown in Fig. 8 is used in every embodiment, and different embodiments include various combinations of the steps (or possibly additional steps than those) shown in Fig. 8. As discussed above, each engineer computer (e.g., engineer computer 110) receives compliance documents, as shown in block 802, which may include auditing or reporting forms. In some embodiments, the engineer computer 110 receives only those parts pertinent to the engineers and/or compliance personnel assigned to that particular engineer computer. Those documents may be received by, e.g., a modem or adapter in the engineer computer 110 that connect the engineer computers to a network (e.g., the Internet). The compliance audits are performed by compliance personnel who may be part of the company or who may be external to the company. In some embodiments, the engineers themselves perform the audit. In either scenario, the engineer computer 110 enables those performing the audit to access compliance documents on-site (e.g., while at a plant in a remote jurisdiction).

[0059] In some embodiments, the compliance personnel and/or engineers may access the compliance documents on hand-held devices (e.g., engineer computers 110, 112, 114) and use those same devices to perform the audit and complete the audit or reporting forms, as shown in block 804. The engineer computers 110, 112, 114 may be tablets, smart phones, or any other portable electronic device that the engineers use to input data on-site. In other embodiments, the engineer computers 110, 112, 114 may be desktop computers or other non-portable computing devices. Completing the audit or reporting forms may include capturing photographs or entering other evidence as required by the compliance documents. Once each engineer has input the required information, the engineer computers 110, 112, 114 transmit the compliance documents and/or completed audit forms back to the compliance computer 108, as shown in block 806. That information may be transmitted and/or received over wired and/or wireless connections to the network. That data may be used to file forms with the local authorities (either by the local

plant managers or by the compliance officer who receives the data from the hand-held devices over the Internet). That data may also be used to complete internal corporate compliance forms.

[0060] In some embodiments, inputting the compliance data and completing the auditing forms is done automatically. For example, the satellite office may employ systems designed to detect and measure CO₂ emissions. That information may be stored at the engineer computers 110, 112, 114 (or on local servers connected to the engineer computers) and used to automatically complete the auditing forms. The engineering computers 110, 112, 114 may also be configured to automatically compare the compliance data with the standards set by the updated compliance documents. In some embodiments, those systems assist local personnel in inputting the compliance data and comparing the compliance data with the standards set in the updated compliance documents. For example, the engineering computers 110, 112, 114 may prompt the local personnel to input the data in a specific format or may automatically verify that the data is within the boundaries set by the pertinent rules.

[0061] Various modifications and additions can be made to the exemplary embodiments discussed without departing from the scope of the present invention. For example, while the embodiments described above refer to particular features, the scope of this invention also includes embodiments having different combinations of features and embodiments that do not include all of the described features. Accordingly, the scope of the present invention is intended to embrace all such alternatives, modifications, and variations as fall within the scope of the claims, together with all equivalents thereof.

CLAIMS

We claim:

1. A computer-implemented method for a first entity to receive, from a second entity, an update to a compliance rule referenced in a compliance document of the first entity, the method comprising:

analyzing the compliance document of the first entity using one or more processors in order to identify a reference to the compliance rule in the compliance document of the first entity and a section of the compliance document in which the compliance rule is referenced;

creating metadata identifying the reference to the compliance rule and the section of the compliance document in which the compliance rule is referenced;

creating a transmission object by the one or more processors by incorporating the metadata identifying the reference to the compliance rule and the section of the compliance document in which the compliance rule is referenced without incorporating the compliance document into the transmission object;

sending the transmission object by the one or more processors to the second entity that uses the metadata identifying the reference to the compliance rule in the compliance document to identify an update to the compliance rule and that compiles the update to the compliance rule into a notification along with the metadata from the transmission object identifying the section of the compliance document in which the compliance rule is referenced; and

receiving, from the second entity in response to the step of sending the transmission object, the notification identifying the update to the compliance rule and the section of the compliance rule in which the compliance rule is referenced.

2. The method of claim 1, wherein the metadata in the transmission object identifies a set of jurisdictions and a set of topics.

3. The method of claim 1, wherein the update to the compliance rule is a modification to the compliance rule, and wherein the method further comprises:

using the notification identifying the section of the compliance document in which the compliance rule is referenced to locate that section; and

updating the compliance document by incorporating the modification into that section of the compliance document.

4. The method of claim 1, further comprising:

receiving a template containing a prompt for information relating to the compliance rule, wherein the information includes jurisdictions in which the first entity operates or a topic of operations for the first entity; and

using the information prompted by the template to create the compliance document for the first entity by generating the reference to the compliance rule in the section of the compliance document.

5. The method of claim 1, further comprising:

creating a profile that identifies an area of operations for the first entity;

transmitting the profile to the second entity; and

receiving a template from the second entity, wherein the template includes a prompt to input the reference to the compliance rule into particular sections of the compliance document, and wherein the prompt is based on the area of operations identified in the profile; and

inputting the reference to the compliance rule into the particular sections of the compliance document.

6. The method of claim 5, wherein the compliance document includes instructions on how the first entity responds to a violation of the compliance rule, wherein creating the transmission object by incorporating the metadata excludes those instructions from the transmission object.

7. A computer-based system for receiving updates to a compliance rule referenced in a company compliance manual while preserving privacy with respect to company-specific compliance policies in the compliance manual, the system comprising:

one or more processors;

an incorporation module configured to use the one or more processors to:

parse a citation to a compliance rule in the company compliance manual from company-specific compliance policies regarding the compliance rule in the company compliance manual; and

create a transmission object that includes the citation to the compliance rule in the company compliance manual without including the company-specific compliance policies regarding the compliance rule from the company compliance manual;

a review module configured to use the one or more processors to present the citation to the compliance rule in the transmission object to a user for approval;

a communications module configured to send the transmission object to an entity responsible for receiving the transmission object, using the citation to identify updates to the compliance rule, and compiling the updates to the compliance rule into a notification; and

an update module configured to use the one or more processors to receive the notification from the entity in response to sending the transmission object, the notification conveying an update to the compliance rule in the company compliance manual.

8. The computer-based system of claim 7, further comprising:

a compliance manual search module configured to search the company compliance manual for references to the compliance rule; and

a compliance manual tagging module configured to create metadata associated with references identified by the compliance manual search module.

9. The computer-implemented method of claim 8, wherein the only data that are incorporated into the transmission object are the created metadata associated with the compliance rule.

10. A computer-implemented method for updating a compliance document with respect to regulatory changes without exposing potentially sensitive information in the compliance document, the method comprising:

analyzing a compliance document of a first entity by one or more processors within a computer system of the first entity, wherein the compliance document includes a citation to at least one compliance rule at a specific location in the compliance document and at least one policy specific to the first entity regarding its compliance with the compliance rule, and wherein analyzing the compliance document includes:

parsing the at least one policy specific to the first entity in the compliance document from the citation to the compliance rule in the compliance document; and

identifying the specific location of the citation in the compliance document;

creating a transmission object by the one or more processors within the computer system of the first entity by compiling the citation to the compliance rule from the compliance document and the specific location of the citation in the compliance document into the transmission object without including the at least one policy specific to the first entity from the compliance document;

sending the transmission object by the one or more processors within the computer system of the first entity to an operator server of a second entity, wherein the operator server of the second entity is configured to analyze the transmission object to extract the compliance rule in the transmission object, search an operator server database to identify an update to the compliance rule, analyze the transmission object to extract the specific location of the citation in the compliance document, and compile the update and the specific location of the citation in the compliance document into a notification;

receiving the notification from the operator server of the second entity by the one or more processors within the computer system of the first entity in response to sending the transmission object to the operator server of the second entity, the notification including the update to the compliance rule from the operator server of the second entity and the specific location of the citation in the compliance document; and

updating the compliance document of the first entity by the one or more processors within the computer system of the first entity using the update to the at least one compliance rule and the specific location of the citation in the notification from the operator server of the second entity.

11. The computer-implemented method of claim 10, wherein the at least one policy specific to the first entity contains at least one of the following: instructions from the first entity on how to respond if the first entity is not in compliance with the compliance rule; guidelines from the first entity for ensuring compliance with the compliance rule; statements from the first entity regarding prior actions with respect to compliance with the compliance rule; and employee identification of employees of the first entity.

12. The computer-implemented method of claim 10, wherein the at least one policy regarding the compliance rule includes a first policy pertaining to a first satellite location regarding the compliance rule and a second policy pertaining to a second satellite location regarding the compliance rule, wherein the first policy and the second policy differ.

13. The computer-implemented method of claim 10, further comprising a step of creating the compliance document by the one or more processors within the computer system of the first entity, the computer system being configured to maintain that compliance document away from external websites.

14. The computer-implemented method of claim 10, wherein the compliance document is a compliance manual.

15. The computer-implemented method of claim 1, wherein the metadata identifying the section of the compliance document in which the compliance rule is referenced is human-readable metadata.